02_hj23_edit 8-04-2003 10:07 Pagina 2

Anno 2 - N. 23
10 / 24 Aprile 2003

**Boss:** theguilty@hackerjournal.it

**Editor:** grand@hackerjournal.it,

**Contributors:** Bismark.it, Antonio Benfante, CAT4R4TTA, DaMe`, Roberto "decOder" Enea, KoRn, {RoSwElL}, Paola Tigrino

**DTP:** Cesare Salgaro

**Graphic designer:** Dopla Graphic S.r.l. info@dopla.com

**Publishing company**
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

**Printing**
Stige (Torino)

**Distributore**
Parrini & C. S.PA.
00189 Roma - Via Vitorchiano, 81-
Tel. 06.33455.1 r.a.
20134 Milano, viale Forlanini, 23
Tel. 02.75417.1 r.a.
Pubblicazione quattordicinale registrata al Tribunale di Milano il 25/03/02 con il numero 190.
Direttore responsabile Luca Sprea

Gli articoli contenuti in Hacker Journal hanno uno scopo prettamente didattico e divulgativo. L'editore declina ogni responsabilita' circa l'uso improprio delle tecniche e che vengono descritte al suo interno. L'invio di immagini ne autorizza implicitamente la pubblicazione gratuita su qualsiasi pubblicazione anche non della 4ever S.r.l.

**Copyright 4ever S.r.l.**
Testi, fotografie e disegni, pubblicazione anche parziale vietata.

**HJ: INTASATE LE NOSTRE CASELLE**

Ormai sapete dove e come trovarci, appena possiamo rispondiamo a tutti, anche a quelli incazzati.

redazione@hackerjournal.it

**hack·er (hãk'∂r)**

*"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."*

# GUERRE PREVENTIVE

**Quella in corso in Iraq è la prima vera "guerra preventiva" della storia contemporanea. Ma anche su Internet e nel campo del diritto d'autore, la strategia sembra la stessa: colpire tutti in modo indiscriminato per punire solo qualcuno.**

### GUERRA ALLA PIRATERIA AUDIO

**La minaccia:** milioni di brani musicali circolano in forma digitale sui network peer to peer, e questo limiterà le vendite di CD (non è vero, ma lasciamo perdere).

**La strategia delle Major:** introdurre sistemi di protezione anticopia nei CD audio, che facciano in modo che il CD venga riprodotto dai lettori "domestici" ma non da quelli dei computer. In questo modo non sarà possibile estrarre l'audio e convertirlo in Mp3.

**I danni collaterali:** non posso più usare il mio computer per riprodurre un CD regolarmente acquistato. Molti normali lettori di CD non riescono a riprodurre i CD protetti, sebbene non siano lettori "per computer". Non posso più effettuare una copia personale di un CD regolarmente acquistato, diritto che mi è garantito dalla legge, ma vietato dalla tecnologia.

**Esito del conflitto:** le protezioni anticopia sono state aggirate nel giro di giorni. Anche chi possiede CD originali, li duplica per poterli usare liberamente con il lettore che preferisce. Oppure, evita di comprare il CD che non funzionerebbe col suo lettore, si scarica gli Mp3 da Internet e li masterizza.

### GUERRA ALLA PIRATERIA AUDIO/2

**La minaccia:** milioni di brani musicali circolano in forma digitale sui network peer to peer, e questo limiterà i ricavi dei diritti d'autore.

**La strategia della SIAE:** far fare al governo una legge che imponga una pesante tassa (fino al 120% del prezzo reale) su ogni supporto vergine (CD-R, VHS vergine, DVD-R) e apparato di registrazione (masterizzatore, videoregistratore). I soldi raccolti andranno versati alla SIAE, che li ridistribuirà coi suoi metodi imperscrutabili.

**I danni collaterali:** chi fa backup su CD, distribuisce software libero o di propria produzione, fa un filmino delle vacanze, sarà obbligato a dare soldi a Dalla e Morandi (e qualcun altro).

**Esito del conflitto:** Dalla e Morandi (e qualcun altro) saranno più ricchi. Tutti noi, un po' più poveri. Ai veri pirati musicali, non cambia nulla: tanto alzeranno il prezzo della copia per recuperare il costo del supporto.

### GUERRA ALLA PEDOPORNOGRAFIA

**La minaccia:** su Internet vengono distribuiti filmati e immagini che ritraggono bambini abusati sessualmente. Da pratica di nicchia, relegata a siti illegali spesso residenti all'estero, rischia di trasformarsi in fenomeno di massa: la parola "lolita" è tra le più gettonate sui motori di ricerca; viene persino prima di "viaggi" e "film".

**La strategia del Parlamento:** ideare una legge che imponga ai provider di connettività di dotarsi di filtri e strumenti in grado di impedire ai minori la visualizzazione di contenuti pornografici (scrivo "Parlamento" e non "Governo" perché anche l'opposizione ha presentato una proposta di legge simile).

**I danni collaterali:** tutti quelli che sanno qualcosa di tecnologia, capiscono al volo che i nostri politici sono completamente ignoranti in materia, perché sarebbe come imporre a Telecom di filtrare tutte le parolacce dalle telefonate. Tutti quelli che sanno qualcosa di politica, intuiscono che è già partita la prossima campagna elettorale.

**Esito del conflitto:** la proposta non diventerà legge, ma intanto si sarà speso un sacco di tempo e denaro per studiare una legge impraticabile, invece di cercare di fermare la produzione di quel materiale ripugnante.

*grand@hackerjournal.it*

03_05_hj23_posta 8-04-2003 10:10 Pagina 3



IL CORAGGIO DI OSARE: INDIPENDENTI DA TUTTI

# Hackerjournal.it, il muro per i tuoi graffiti digitali

w w w . h a c k e r j o u r n a l . i t

## SCRIVI PER HJ!

Siamo sempre alla ricerca di nuovi collaboratori, per rendere HJ sempre più bello e interessante. Non ci interessano tanto le guide o i corsi a puntate su un linguaggio (piuttosto, realizzate un articolo su come iniziare a programmare un linguaggio, e dove si trovano le guide più interessanti in Rete). Vogliamo articoli in cui si spiega come spremere al massimo la tecnologia che abbiamo a disposizione. O meglio, usarla per scopi diversi da quelli per cui è stata realizzata :-)
Date sfogo alla fantasia, e parlate di come forwardarvi alcune email sul cellulare, di come trasformare un client di posta in un fileserver, come creare un riproduttore di Mp3 per l'auto con un vecchio PC, di come usare il frullatore come ventola per il processore…
Per saperne di più su lunghezza e formati di file, mandate una mail a grand@hackerjournal.it con "FAQ Articoli" come soggetto.

## Nuova password!

Ecco i codici per accedere alla Secret Zone del nostro sito, dove troverete informazioni e strumenti interessanti. Con alcuni browser, potrebbe capitare di dover inserire due volte gli stessi codici. Non fermatevi al primo tentativo.

user: **qualc1**
pass: **barz8**

## ALCUNI ARTICOLI INTERESSANTI...

Ecco alcuni degli articoli apparsi di recente su Hackerjournal.it .Protezioni anticopia? solo perdita di soldi e brutte figure. Alcuni sistemi per la protezione della copia di CD audio. Spamming e finestre attive!
Vi siete ritrovati finestre aperte con messaggi pubblicitari senza aver cliccato niente? Può essere un baco di MSN Messenger: scoprite come risolverlo. JAVA per Linux, Limewire e Mozilla Installare e aggiornare Java sul pinguino.

## I NOSTRI/VOSTRI BANNER!

Nel momento in cui scriviamo, siamo arrivati a ben 88 banner realizzati da voi e pubblicati sul sito di HJ. Ecco i più belli di questo numero:

## Dai bit alla carta

# mailto:

redazione@hackerjournal.it

## EFFETTI COLLATERALI

Gentile redazione di HJ, vi leggo dal n° 6, trovo i vostri articoli spesso utili e sempre interessanti. Purtroppo non vi leggerò più: le persone a me più vicine e più care insistono a dire che da quando leggo regolarmente il vostro periodico sto diventando molto strano, dico cose senza senso e non ho più il senso della realtà. Io non capisco cosa vogliono dire e mi rivolgo a voi in cerca di consiglio, raccontandovi a titolo di esempio la giornata di ieri.

Mi alzo alle 7 e apro la porta 25 per scaricare il giornale dal server delle news "zerbino", gli do un'occhiata e lo archivio nelle librerie poi apro le windows per cambiare l'aria. Avendone accertato scadenza e provenienza puccio i cookies nella CoffeeCup. Chiudo casa a doppia chiave e mando un pacchetto echo all'ascensore ma non ottengo risposta quindi scendo a piedi e incontro il più figlio di trojan tra gli utenti del conDomain; cerco di mascherare il mio ip ma è tutto inutile, lui mi scaglia addosso uno spike e mi prende in pieno, provo a disconnetterlo e reagisce con un flood verbale che mi manda in patience overflow, allora me lo levo di torno con la bruteforce e arrivo dal portinaio: questi dice che ho subito dei cambiamenti e non mi da accesso alla rete stradale, "mi sono tagliato la barba, cretino!" Mi fa passare: salgo in auto, clicco col destro sull'autoradio, e overclocco a manetta il condizionatore per rinfrescare il pinguino. Arrivato in office incontro una client nuova: Mi colpiscono subito le sue 2peer ma analizzo anche l'elegante cintura di python, proverei subito un attacco in backdoor, ma lei si accorge del mio portscanning ed erge un robusto firewall. Klez!!!!

In pomeriggio con un unexpected popup spunta il capo e mi inoltra una perentoria query di accompagnarlo in sede. Devo rifornire l'auto col GPL ma lui ha un meeting con high priority, perciò devo pigiare sull'accelerator plus che mail: rischio due crash ma fortunatamente non troviamo queque e arriviamo in time to live.

La sera in proxy dell'auto c'è un vigile: cerco di convincerlo a decompilare la multa, a chiudere o almeno ridurre a icona un occhio.. Sembra inflessibile quando "ICQ!!" starnutisce improvvisamente, si era beccato un virus: per fortuna avevo una confezione di Norton sciroppo in macchina, la sharo con lui che, grato, rippa la contravvenzione senza nemmeno loggarmi la targa. Tornato alla Home page trovo l'intera community familiare intenta a chattare nella room della tv, dove un orchestrista baffuto dice di chiamarsi Demo.. ma sono stanco, spengo, vado a letto e entro subito in modalità risparmio energetico.

Io non vedo nulla di preoccupante, voi che ne pensate?

**FiloRB**

*ACK! Hai ragione: devi perlomeno suspend la read di HJ. Comunque, I/O ti segno nel registry dei lettori più SMTPatici :-)*

## ☺ Tech Humor ☺

**Non c'è che dire: un modding decisamente "gotico".**

## TRY2HACK KAPUT

Vorrei saper come poter scaricare try2hack visto che il sito ufficiale non dà nessun segnale di vita e neanche da questo sito è possibile scaricarlo.

**Matrixxx**

*Try2hack non si scarica, si gioca on-line. Purtroppo, pare che nell'aggiornare il server i curatori del sito lo abbiano cancellato per errore, e devono ripristinare tutto quanto. Su www.try2hack.nl si legge infatti un promemoria molto ironico "Ricordarsi di fare il backup di try2hack prima di aggiornare la macchina la prossima volta". Promettono anche di rimetterlo online il prima possibile.*

## ANTEPRIMA IN WINMX

Vorrei aggiungere 2 righe all'articolo riguardante WIN-MX, pubblicato qualche tempo fa, in merito al problema di non poter avere un preview del file in fase di dowloading e quindi scaricare per ore... una bufala.

Provate ad andare nella cartella di destinazione del download, cliccate con il tasto destro del mouse sul file interessato (INCOMPLETE_... ) selezionate "Copia" e poi incollatelo da qualche altra parte. A questo punto, sempre col tasto destro, usiamo l'opzione "Rinomina" (assicuratevi di aver disabilitato in -WinZoZ- l'opzione che nasconde le estensioni dei file) e diamo al file un nome con l'estensione propria del file che pensiamo di star scaricando (per esempio, se ci aspettiamo che "INCOMPLETE_...La_fuga..." sia un Mpeg, rinominiamolo in "La_fuga _del cavallo_morto.mpg). Ecco un file che può essere aperto dal lettore multimediale preferito.

**..::FXM::..Gianni ..::**

## VIRUS CHERNOBYL

Il virus Chernobyl brucia veramente la scheda madre,
e se lo fa, come fa? Su che cosa agisce?

**Maurizo**

*Non la brucia, ma può resettare il Bios, rendendola inutilizzabile. In certi casi, è necessario proprio cambiare il chip del Bios per poterla utilizzare di nuovo.*

## TESTARE LA SICUREZZA

Ho un sito Web e ne voglio testare la sicurezza, mi consigliate degli exploit per testare se il mio sito è in pericolo di defacement?

**Luigi M.**

## ☺ Modding ☺

**Un Mac Cube riverniciato dall'interno con sfumature astratte.**

*Puoi usare Nessus (www.nessus.org), da montare su un sistema Unix che effettuerà una serie di tentativi di attacco. I risultati possono essere visti anche da Windows. Attenzione però: se il server non è sotto il tuo controllo (cioè se il sito è in hosting, e non su una tua macchina dedicata), devi chiedere l'autorizzazione del provider.*

*Altrimenti, l'uso di Nessus può essere interpretato come un tentativo di attacco che -anche se effettuato verso il tuo sito- di fatto interessa l'intero computer su cui è ospitato.*

### BOOT DI LINUX DA CD

Per lavoro (sistemista, evviva le reti) devo controllare se le reti dove mi trovo sono ok e di solito uso linux perchè preferisco usare Ethereal, nmap e via discorrendo per scoprire se ci sono host attivi dove non dovrebbero o per vedere se qualcuno ha accesso a risorse che non dovrebbe neppure sapere se esistono (praticamente sono un sysadmin ambulante!!!). Il problema è che al 99,99999% non trovo linux dove sono, quindi mi servirebbe poter creare un cd con linux e le utility che mi servono in modo che mettendo il cd e riavviando il PC con boot da cd io possa utilizzare una linuxbox. Sapete darmi una dritta o almeno qualche riferimento certo?

*Devi usare quella che viene definita una "distribuzione Live", che fa esattamente quello che dici. Esistono versioni Live di alcune famose distribuzioni (per esempio, SuSE da un po' di tempo distribuisce gratuitamente i binari solo all'interno di distribuzioni che funzionano in questo modo), e anche alcune distribuzioni nate esplicitamente con questo scopo. Tra queste, la più completa è probabilmente Knoppix (www.knopper.net/knoppix/index-en.html). La distribuzione base comprende il Kernel 2.4, KDE 3.1, X Multimedia System, GIMP, utility per il recupero dati e l'amministrazione di rete.*

### FINTO BUG IN XP

Credo e sottolineo CREDO di aver trovato un bug su win xp professonal.
Avrei voluto scrivere a quelli della Microsoft, ma poi mi sono detto "perch/fargli un eventuale piacere gratuito, con tutto quello che costano i contratti e tutto il resto?"
Così dato che la vostra simpatia x windows è rinomata ho deciso di avvertire voi.
Per essere sicuro di non dire una caxxata mi sono scaricato tutti gli aggiornamenti e dopo averli installati per benino ho scoperto che si possono ancora vedere i video su Paint! :) Come?
Ecco la ricetta:
Aprite un filmato mpgeg con windows media player e fate una foto dello schermo con il tasto "stamp" .
andate su Paint (senza fermare il video e senza ridurre ad icona) e invece di prendervi una foto dello schermo, vi vedrete tutto il video su Paint! So bene che non è un bug grave però è pur sempre un bug.
Per averlo scoperto un utente normale vuol dire che ce ne sono davvero molti.
C'è una cosa che non capisco, sul mio portatile il bug è presente, sul PC fisso di mio fratello non succede, e sempre sul fisso di un mio amico è ancora presente, come mai questa differenziazione?

**Stealth**

## ☺ Tech Humor ☺

**...c'è anche chi ha trasformato il suo iMac in un vero acquario!**

## ☺ Modding ☺

**L'apoteosi del "vedo e non vedo": un PC trasparente.**

*Di segnalazioni così ne sono arrivate tre quasi uguali con nomi diversi. Mettetevi d'accordo su chi lo ha "scoperto" per primo.*
*In ogni caso, non si tratta esattamente di un bug, ma di un effetto collaterale del meccanismo di funzionamento degli acceleratori grafici. La cosa più o meno funziona così: la cattura dello schermo ha effetto sul normale sistema grafico di Windows. Che però non può sfruttare i più moderni meccanismi di accelerazione hardware.*
*Quando si visualizza un filmato, o un gioco 3d, Windows si limita quindi a visualizzare nella finestra un particolare colore trasparente, lasciando al driver il compito di pilotare direttamente la scheda video.*
*Quando catturi lo schermo coi normali sistemi (print screen), in realtà catturi una finestra riempita di quel colore "trasparente". Che se sovrapposta a un filmato, ti mostrerà la finestra sottostante.*
*Il fatto che su alcuni computer funzioni e su altri no dipende dalla scheda video e dal driver utilizzato. Tutto qui. Nessun baco.*

# NEWS

## HOT!

### I CELLULARI FANNO MALE

I cellulari alla stregua delle sigarette? È la proposta di un parlamentare di Forza Italia, Enrico Nan, che individua e stigmatizza i danni elettromagnetici causati dall'utilizzo di cellulari in ambienti chiusi dalle caratteristiche particolari, come un ascensore. Ma non solo. Denuncia anche vere e proprie nevrosi e altri "danni morali" provocati dall'abuso del telefonino e dall'invadenza dei suoi trilli in treno, nei locali pubblici e in altri luoghi di comune frequentazioni.
Se la legge passerà – e a New York già è così - si parla di multe per gli "untori" oscillanti fra 500 e 1000 euro.

### PROBLEMI CON IIS 5.0

L'ennesima vulnerabilità di buffer overflow è stata individuata in IIS 5.0, che viene installato ed eseguito di default su Windows 2000 Server. Come già in altri casi, questo bug può consentire di controllare la macchina da remoto, problema particolarmente grave nel caso il server Windows 2000 sia un Web server, dato che l'attaccante potrebbe eseguire codice arbitrario all'interno del Local System Security Context.
La patch è disponibile sul sito Microsoft o installabile mediante Windows Upgrade.

### CODERED COLPISCE ANCORA

Windows 2000 non ha pace, in questi giorni. Oltre alla già citata vulnerabilità, si deve annunciare un triste ritorno: CodeRed.F, una variante del già noto e famigerato Code Red II, un trojan che già creò parecchi problemi un paio di anni fa. Anche in questo caso è IIS a essere attaccato, e anche in questo caso la patch è già disponibile. Allo stesso modo i software antivirus non dovrebbero avere problemi a riconoscere il virus, del tutto simile, nel codice, al suo predecessore.

### GLI SCHERZI DI LIBERO

LIBERO

Nel giro di pochi giorni Infostrada, intesa come la "mamma" delle caselle di posta Libero, Iol, Wind e Blu, ha giocato un paio di brutti scherzi ai suoi utenti. Il primo, improvviso e piuttosto catastrofico, consiste nell'aver letteralmente bloccato la comunicazione dei suoi utenti con le liste di Yahoo Groups, questo a causa della presenza di alcuni degli IP di Yahoo! in una diffusa e piuttosto feroce lista antispam, quella curata da Spews.org. Tale lista viene utilizzata – e questo accadimento lo dimostra senza ombra di dubbio – da Infostrada per filtrare sul server i messaggi in arrivo. Ma le conseguenze di questa scelta sono ora molto serie, considerando la diffusione e il numero di iscritti a queste liste. E l'errore 550 che viene restituito agli owner è indiscutibile: "blacklisted IP address". Senza contare che in questo modo gli account di posta che respingono le mail di Yahoogroups vengono sospesi automaticamente dalla lista. Le soluzioni possibili sono due: che Libero faccia un'eccezione, nella blacklist, per gli indirizzi Yahoo (improbabile, nonché pericoloso precedente) o che, piuttosto, Yahoo metta in atto tutte le misure possibili per uscire dalla famigerata blacklist.

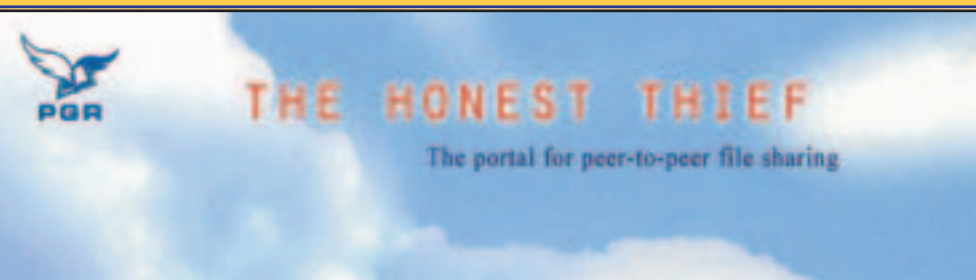
YAHOO! Groups

Il secondo scherzo giocato da Libero ai suoi tanti, affezionati utenti è quello della nuova policy di Digiland, la comunità di siti ospitati gratuitamente dal provider sui propri server. A tutti i gestori di siti è arrivato un messaggio breve ma perentorio che non lascia adito a dubbi: "Gentile cliente, al fine di ridurre sensibilmente il rischio di ospitare contenuti illegali sullo spazio Web di Digiland ti informiamo che, a partire dal 24/03/2003, la pubblicazione o modifica dei contenuti su spazio Web ospitati da Digiland potrà avvenire esclusivamente collegandosi tramite Pop o connessione Adsl Libero, Infostrada o Wind. Qualora, decidessi di cancellare i tuoi contenuti, potrai farlo disabilitando il servizio di spazio web all'indirizzo: http://digiland.libero.it/". Questo con un preavviso a dir poco risibile, visto che la mail in questione è arrivata nel giorno stesso della "scadenza dell'ultimatum". Ed è questa la critica più diffusa fra gli utenti, che non contestano, in linea di massima, il diritto di Libero a riservare ai propri utenti il servizio erogato peraltro gratuitamente, ma la possibilità quasi nulla di intervenire, nel caso si disponga di una connessione in fibra ottica, Adsl differente da quello Infostrada o si acceda a Internet da postazione pubblica.

### MUSICA IN CAMBIO DI TEMPO PROCESSORE

PGR

THE HONEST THIEF

The portal for peer-to-peer file sharing

Una piccola azienda olandese, PGR BV, ha avuto una idea piuttosto originale. Alla ricerca di un sistema per conciliare da una parte le giuste esigenze di guadagno da parte dei musicisti, e dall'altra l'irrefrenabile diffusione della condivisione della musica, ha proposto il servizio The Honest Thief, basato sul software ThankYou, che associa le funzionalità del peer to peer con quelle del grid computing. In parole povere, i computer connessi in Rete per lo scambio dei file mettono a disposizione, come già accade in sistemi come SETI@home, le loro risorse di calcolo inutilizzate, che vanno a formare una sorta di supercomputer virtuale. Secondo gli ideatori del sistema, tale potenza di calcolo avrebbe un valore tale sul mercato da permettere di ripagare le licenze del materiale (musica, video e via dicendo) scambiato nell'ambito del sistema. L'ambizioso progetto, vagamente utopistico, nascosto fra le righe di questo sistema è quello che eliminare completamente il ruolo delle case discografiche, che già vacillano sotto i colpi di Kazaa e WinMX, per creare un sistema del tutto autogestito di distribuzione dei contenuti musicali.

06_08_hj23_newspp 8-04-2003 10:14 Pagina 7

## CENTRINO: IL PROCESSORE È MOBILE

I toni sono trionfalistici e la campagna pubblicitaria massiccia, come non succedeva fin dai tempi del lancio dei primi Pentium: la piattaforma di Intel dedicata al wireless promette di far parlare molto di sé. L'intento, ambizioso ma non irrealistico, è quello di rendere il wireless una funzionalità di base di tutti i computer portatili, e non più un optional per fanatici.

I punti di forza di Centrino sono le dimensioni ridotte, il peso non eccessivo e l'autonomia elevata, nell'ambito di una architettura frutto di studio originale (non, come accade di solito, una rielaborazione delle tecnologie per desktop), che comprende il processore Pentium-M, i chipset i855 e il modulo Wi-Fi 802.11b. Le macchine a cui Centrino è dedicato appartengono a una fascia medioalta, di costo previsto fra i 1500 e i 2500 dollari. Il basso consumo (minore di un watt), ottenuto grazie a tecnologie di modificazione dinamica della tensione del chip, si associa a una velocità di clock non elevatissima (1,6 GHz al massimo), nell'ambito però di una architettura ottimizzata, in grado di eseguire più istruzioni nello stesso ciclo di clock rispetto a un Pentium 4.

### I RIVALI: TRANSMETA

Transmeta, piccola azienda californiana, non teme il gigante Intel, e scende in competizione con il suo Crusoe TM8000, che vuole sfidare direttamente il Pentium-M, meglio noto col vezzoso nome di Centrino. La società è esclusivamente specializzata nella produzione di processori a basso consumo, ed è facile comprendere quanto si senta minacciata dall'arrivo del nuovo processore. Anche Transmeta punta, oltre che sul risparmio energetico, sulle dimensioni ridotte e sulla massimizzazione del numero di istruzioni per ciclo di clock. La sfida vera e propria è però sui bassi costi di produzione: questo permetterà di implementare il Crusoe TM8000 sui notebook a basso prezzo, quelli attorno ai 1000 dollari, al contrario di quello che prevede la politica di Intel nei confronti di Centrino, che, come già detto, sarà riservato a una fascia di prezzo superiore.

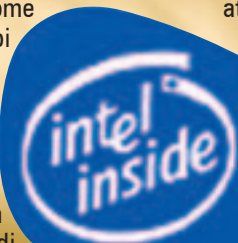
Per quanto riguarda le memorie, lo standard supportato è il DDR400, ma è assicurata la compatibilità verso DDR266 e DDR333; lo standard grafico è AGP4x.

Il processore dovrebbe essere commercializzato nel corso del terzo trimestre 2003.

### E AMD NON STA A GUARDARE

AMD non poteva restare fuori dalla lotta per il mercato delle Cpu per dispositivi mobili, e annuncia il lancio sul mercato di un numero non indifferente di processori dedicati. Ovviamente, intende sfidare quelli che sono i punti di forza già messi sul tappeto da Intel e il piccolo ma specializzato rivale Transmeta: peso e dimensioni ridotte, ottimizzazione dei cicli di clock e consumi energetici ridotti. Ma non l'implementazione del wireless, non per ora, almeno: la scelta di AMD è quella di offrire compatibilità agli standard più diffusi, lasciando fuori dal chip il supporto wireless. A differenza di Intel, peraltro, AMD ha continuato a derivare i suoi processori wireless da quelli per desktop, limitando quindi le possibili implementazioni innovative, e soprattutto non riuscendo a rivaleggiare con i bassissimi consumi energetici dei rivali.

I modelli Athlon XP-M previsti si dividono in due categorie: quelli rivolti in particolar modo ai portatili ultrasottili e ultraleggeri, 1800+, 1700+, 1600+, 1500+ e 1400, e quelli per i notebook tradizionali di fascia medio-elevata, 2600+, 2500+, 2400+, 2200+ e 2000+.

## HOT!

### WEBCAM IN MESSENGER

Microsoft ha finalmente implementato il supporto della webcam nella nuova versione di MSN Messenger 5.0. Gli host di stream sono forniti da Logitech, e permetteranno di comunicare in video in tempo reale. Questa è una miglioria interessante non solo per chi utilizza l'instant messenger per tenersi in contatto con gli amici e fare nuove conoscenze, ma anche per quella fascia di utenti sempre più nutrita che ha implementato gli instant messenger in un ambito aziendale.

### LA LAVATRICE CHE PARLA

Per ora è solo un prototipo, ma chissà in quanti la aspettano con ansia: stiamo parlando della lavatrice parlante Hermine, prodotta dall'azienda tedesca Speech Experts in collaborazione con Siemens. Hermine è in grado di riconoscere una serie di comandi vocali, venendo così in aiuto degli utenti poco esperti: basterà dire alla lavatrice che tipo di abiti vogliamo lavare, e lei ci dirà quale programma utilizzare, aggiungendo anche commenti spiritosi sulle macchie. Se la risposta del pubblico sarà favorevole, Hermine potrebbe già essere commercializzata a partire dall'anno venturo.

### I VINCITORI DELLE OLIMPIADI INTERNAZIONALI DELL'INFORMATICA

Ci sono stati 42 premiati, su oltre 7500 partecipanti alla selezione italiana di questa peculiare competizione, che si è svolta a Bologna. L'iniziativa è dell'UNESCO, e in Italia è sponsorizzata dall'Associazione Italiana per l'Informatica e il Calcolo Automatico e il ministero dell'Istruzione. La competizione è rivolta agli studenti della scuola media superiore di età compresa fra i 15 e i 20 anni. I primi tre classificati sono stati Stefano Maggiolo di Padova, Stefano Soffia di Reggio Emilia, e Andrea Bergia di Fossano, in provincia di Cuneo.

# NEWS

HOT!

## NICEHELLO, NOT SO NICE

Un virus che attacca principalmente gli utenti "casalinghi" e gli utenti di Hotmail che utilizzano MSN Messenger si sta diffondendo in questi giorni. Si tratta di W32/Nicehello@MM, ed è incorporato in quello che apparentemente è una piccola applicazione Flash, accompagnata da un commento in lingua spagnola. Una volta eseguito, mostra un errore fittizio e si autoinvia a tutti i contatti Hotmail della propria lista di utenti del messenger, inviando all'autore del virus il proprio username e password.

## UN GIRO DI VITE AGLI MMS

Attenzione alle foto fatte col cellulare: non cerchiamo di emulare le varie pubblicità, rubando foto qua e là senza chiedere il permesso a chi è ritratto. Vero che i risultati, al contrario di quel che si vede nelle succitate pubblicità, non sono certo lusinghieri, e spesso è difficile che la gente si riconosca nelle sgranate immagini MMS. Ma non corriamo ugualmente rischi. Gli MMS sono del tutto paragonabili a immagini fotografiche ordinarie, quindi sono soggette alle leggi vigenti, che non sono poche: una cosa è mandarli ad amici e parenti o comunque guardarli e cancellarli, altra cosa è giocare a 007, mandandoli a catene interminabili di utenti o pubblicandoli in Rete, magari gongolando per la brutta figura che stiamo per far fare alla persona ritratta in una situazione imbarazzante. Le immagini diffondibili sono quelle per cui la legge considera ci sia una implicita autorizzazione alla base, come quelle di personaggi pubblici in situazioni pubbliche. Non parliamo neppure delle immagini catturate all'interno di una abitazione, o peggio ancora osè, per cui le cose si complicano ulteriormente, soprattutto se inviate a minori.

## MOZILLA SI RINNOVA

mozilla.org

E' disponibile la versione 1.3 del celebre browser open source, che è spesso al centro di polemiche più o meno divertenti (si ricordi il recente episodio della Bork Edition), e in occasione di questa sua ultima release non ha smentito la sua tradizione: un diffuso settimanale italiano ha stigmatizzato il suo logo, il simpatico lucertolone che compare in una stella, avvicinandolo alla stella a cinque punte di triste memoria brigatista rossa, e facendo diventare la mascotte di Mozilla un tirannosauro. Facezie a parte, vediamo quali sono le novità di rilievo presenti nella nuova versione, o meglio, cosa è stato potenziato. In effetti non c'è nulla di davvero nuovo, ma sono presenti parecchie migliorie, fra cui i filtri, che sono ora "addestrabili", in modo da esercitare un controllo antispam più minuzioso sulla posta in arrivo, e possono inoltre permettere di classificare i messaggi presenti nei newsgroup.
Le immagini sono ora ridimensionate in automatico nella finestra del browser, come accade in Internet Explorer, e in generale è stata migliorata l'aderenza agli standard e la compatibilità coi siti Web.
La nuova versione del browser è disponibile per Macintosh, Windows, Linux, OpenVMS, Solaris 8, AIX e HP-UX.

## SMARTPHONE E NON SOLO

Sony Ericsson P800 è un cellulare pieno di risorse, a tal punto che quasi ci si dimentica che serve anche per telefonare. E questo è male, visto che supporta lo standard triband per telefonare nei paesi che non supportano i nostri protocollo Gsm – come gli Stati Uniti. Oltre a questo, troviamo uno schermo a colori piuttosto ampio e con una buona risoluzione, fotocamera digitale, player MP3 e MPEG, browser Web, posta elettronica e organizer sincronizzabile con il Pc. Inoltre dispone di una gamma di giochi di buona qualità, il supporto alle Memory Stick, una tastierina a schermo per inserire i dati mediante lo stick accluso e l'ottimo sistema operativo Symbian.
Il costo è di 800 euro circa, non eccessivo per un simile prodotto.
L'unico vero problema è riuscire a trovarlo: fin da quando è stato disponibile, poco dopo Natale, è molto difficile trovare negozi che lo abbiano a disposizione o che, per lo meno, siano in grado di procurarlo in tempi brevi.

## VESTITI RADIOCONTROLLATI

Benetton ha intenzione di fornire di un piccolo radiochip, in tecnologia RDIF (Radio Frequency Identification), marchiato Philips, tutti gli abiti che mette in vendita nei propri negozi, per migliorare la gestione del magazzino e "tracciare" la strada percorsa dai vari capi. Non si tratta di una novità assoluta, in quanto grande industrie automobilistiche e di elettronica nordamericane hanno già da tempo in uso lo stesso sistema, ma trattandosi di capi di abbigliamento era inevitabile, come è stato, una sollevazione da parte delle associazioni dei consumatori, che vedono in questo radiochip una possibile minaccia alla privacy.

NIENTE GUERRA SULLE RADIO INGLESI, E AL JAZEERA FUORI DAL WEB

# PROPAGANDA E CENSURA

## E' l'informazione in tempo di guerra, baby...

Dal termine della barbarie del nazismo, gran parte del mondo ha fatto molti passi in avanti verso la conquista di **diritti che ormai consideriamo fondamentali, irrinunciabili, e acquisiti per sempre**. Ma siamo sicuri? Per esempio, una cosa di cui in tanti eravamo convinti era che **nessun paese occidentale avrebbe mai potuto attaccare un paese straniero senza provocazione**. E che, nel caso fosse successo, in un mondo interconnesso, **non si sarebbe potuta spegnere la voce di milioni di persone contrarie a tutto ciò**. Pensavamo che la parola "censura" fosse ormai cosa del passato, oppure una pratica adottata solo da paesi retti da una dittatura. E soprattutto, che **per lo meno su Internet non fosse possibile censurare niente**.

## >> Blair killed radio stars

E invece, il 25 marzo si è saputo che l'autorità delle comunicazioni inglese ha **vietato a radio e tv, pubbliche e private, di trasmettere canzoni e video clip che parlino di guerra**, o che anche lontanamente abbiano qualcosa a che fare con essa. Oltre ai testi più esplicitamente pacifisti, radio e tv stanno mettendo al bando anche il repertorio dei B52's (per via del nome del gruppo), video che ritraggano soldati o scene di guerra, **e già che ci sono, prendono la palla al balzo e censurano anche Sunday Bloody Sunday degli U2 e Zombie dei Cranberries**, che parlano delle violenze degli Inglesi in Irlanda del Nord.

## >> La Rete è ancora libera?

Neanche Internet scampa dalla censura, anche se avviene in modi più subdoli. Per esempio accade che Salam Pax (autore del blog Dear Raed dove affronta la situazione attuale dal punto di vista di un iracheno contrario a Saddam, ma critico verso l'intervento USA, http://dear_raed.blogspot.com) si sia visto **sostituire le foto pubblicate sul blog con vignette umoristiche**. Inizialmente si è pensato all'attacco di un defacer, ma poi si è scoperto che a operare la sostituzione (o meglio, il redirect verso un altro sito), è stato **il proprietario del servizio di hosting**. Si è ritrovato la banda congestionata dalle migliaia di accessi che Dear Raed ha avuto dagli inizi del conflitto, e ha agito a modo suo segando il materiale scomodo. Fortunatamente, questa situazione si è risolta grazie a Blogspot, che ha deciso di ospitare gratuitamente le immagini di Dear Raed. Ma il giallo si amplia: mentre scrivo, sono alcuni giorni che non si hanno notizie di Salam Pax, che ha smesso di aggiornare il blog. Paura.

## >> Cracker o militari?

Il giorno dopo, il sito di Al Jazeera, emittente tv in lingua araba che da poco ha inaugurato una sezione in inglese, **risulta inaccessibile**. Anche se il traffico generato nelle prime ore è stato effettivamente superiore alle aspettative, non si tratta di un semplice effetto Slashdot amplificato su scala mondiale: **qualcuno ha portato un attacco DOS e ha inoltre modificato i valori di Aljazeera.net nella tabella del DNS**. Il pratica, l'emittente ha perso il controllo sul dominio aljazeera.net.Sono stati degli hacker patriottici arrabbiati perché Al Jazeera è vicina alle posizioni del nemico? Servizi segreti americani che vogliono spegnere una voce incontrollata? Hacker assoldati dalla CIA, magari in cambio di una "pulitina" alla fedina penale? **Non lo so e non me ne frega niente.** Quel che mi preoccupa è che, nel terzo millennio, qualcuno possa con la forza privarmi di un mio diritto all'informazione. Che se non hai soldi per permetterti server sovradimensionati (o servizi come quelli di Akamai.com, specialista nella gestione di traffico elevatissimo), **la tua voce non sarà sentita, nemmeno su Internet.**

Qualche giorno prima qualcuno è riscito ad entrare anche nel sito della casa bianca, ma la cosa ha fatto molto meno rumore... Come mai secondo voi?

grand@hackerjournal.it

PS: Oh, intendiamoci. Non penso che Al Jazeera dica la verità assoluta. Ma siccome penso la stessa cosa anche di CNN, Fox News, TG 5… TG 4… 3… 2… 1… (boom, Studio Aperto!), è importante poter sentire tutte le campane per farsi un'opinione.

LE NUOVE DIRETTIVE EUROPEE RENDONO ILLEGALE IL NETSTRIKE

# CORTEI

**A fine Febbraio, i Ministri dei diversi Paesi dell'Unione che compongono il Consiglio Europeo della Giustizia hanno avviato "una direttiva che equipara spammer, netstriker e terroristi informatici sotto l'unica definizione di coloro che inviano materiale elettronico non richiesto".**

Se ne è discusso in Italia (Punto-Informatico e Zeus-News) e sul The New York Times il cui articolo di Paul Miller del 5 Marzo 2003 chiarisce, già nel titolo, cosa accadrebbe se tale direttiva ricevesse consensi: "Europe Hacker Laws Could Make Protest a Crime" (Le leggi europee sugli hacker potrebbero rendere la protesta un crimine). Sebbene ci sia la possibilità di una revisione e modifica, vi racconteremo comunque quali reazioni ha suscitato la notizia e, nel contempo, cogliamo l'occasione per parlarvi di Netstrike, proporvi letture e approfondimenti, sperando che riflettiate ancora una volta sui principi etici dell'hacking e su come questi stessi principi possano essere applicati anche al di fuori del mondo dei computer.

## >> Nuove leggi

In base alla direttiva dell'UE, sarebbero considerati "criminali" non solo coloro che rendono la nostra casella e-mail un vero e proprio contenitore di spazzatura, inviandoci, contro la nostra volontà, pubblicità di prodotti e siti web (spammer). Non solo coloro che scrivono e diffondono virus informatici o che penetrano illegalmente in un sistema informatico protetto, alterando, modificando o danneggiando i dati contenuti in esso (crackers). Per costoro – è bene ricordarlo - se facenti parte di un'organizzazione criminale o terroristica, è prevista una **pena fino a 5 anni di carcere (in USA addirittura l'ergastolo)**; mentre per la ragazzata di qualche genietto del computer, forse per il web defacing, che come sappiamo consiste nella sola modifica di una home page, in ogni caso per qualsiasi azione isolata la pena è al di sotto dei tre anni e al di sopra di uno (dipende dal tipo di danno commesso). **Sarebbero considerati "criminali" persino coloro che protestano via Internet**, coloro che partecipano ad iniziative pacifiche di contestazione web, come quella contro la guerra in Iraq che di recente ha invitato a mettere in difficoltà il sito della Casa Bianca inviando in massa messaggi di posta elettronica (netstriker).

## >> Cos'è il netstrike

Protestare potrebbe insomma essere considerato un "crimine"!! Il netstrike, infatti, altro non è che una forma di protesta, una pratica di mobilitazione in rete, **nata nel 1995 dall'associazione culturale StranoNetwork** (www.strano.net) e dalla proposta di T.Tozzi di utilizzarla come forma di opposizione agli esperimenti nucleari francesi di Mururoa. Da allora sono stati effettuati vari netstrike – contro la pena di morte, ad esem-

### HACKTIVISMO!

Il termine Hacktivism, per chi fosse ignaro del fenomeno, nasce dall'unione – citiamo qui Di Corinto e T. Tozzi, - di "hacking", «inteso come quella particolare attitudine verso le macchine informatiche che presuppone sia lo studio dei computer per migliorarne il funzionamento - attraverso la cooperazione e il libero scambio di informazioni tra i programmatori - sia la condivisione del sapere che ne risulta per dare a tutti accesso illimitato alla conoscenza in essi incorporata», e il termine americano "activism", con cui si indicano «le modalità dell'organizzazione e della propaganda politica proprie dei movimenti politici di base (grassroots movements) e le forme di azione diretta come sit-in, cortei, picchetti, boicottaggio delle merci e dei consumi, occupazione di stabili e di strade, autogestione degli spazi e autoproduzione di beni, merci e servizi». L'attivismo sociale e la militanza politica hanno col tempo adottato l'etica e le tecniche proprie della cultura hacker, cosicché "dai volantini si è passati alle petizioni elettroniche e dalle manifestazioni di piazza ai sit-in elettronici". Per Hacktivism deve intendersi un uso non convenzionale del computer, finalizzato a migliorare il mondo, e in particolare le condizioni di libertà, di uguaglianza e di fratellanza tra i popoli, sia "dal basso", all'interno dei movimenti sociali, nei collettivi politici, nell'underground artistico, sia attraverso un modello di reti telematiche.

pio, e l'invasione del Chiapas da parte dell'esercito messicano. Per saperne di più basta dare un'occhiata a www.netstrike.it, il sito che diffonde informazione sui netstrike passati, presenti e futuri. Di cosa si tratta esattamente? Un netstrike può essere immaginato come "la trasposizione in rete di un sit-in pacifico". La metafora che meglio lo rappresenta "è quella di un consistente numero di persone che attraversano una strada su un passaggio pedonale, munite di cartelli e striscioni e che se il loro numero è veramente consistente possono arrivare a bloccare il traffico per un determinato periodo di tempo" (www.ecn.org/inr/netstrike). Più propriamente trattasi di un "corteo telematico" (il termine in italiano non va infatti tradotto letteralmente come 'sciopero telematico'), che **"consiste nell'invitare una massa considerevole di utenti possessori di accessi Internet e browser a puntare i propri modem verso uno specifico URL a una precisa ora e ripetutamente. In questo modo viene occupato un sito web fino a renderlo inutilizzabile, almeno per la durata della mobilitazione"** (www.netstrike.it/index2.html).

## >> Dubbi sulla punibilità

Tra gli esponenti della nostra classe politica che hanno espresso perplessità riguardo alla direttiva dell'UE, ricordiamo, per la cronaca, il senatore verde Fiorello Cortiana, il primo firmatario della proposta di legge per l'adozione del Software Libero nella Pubblica Amministrazione italiana e il parlamentare europeo Marco Cappato, Presidente della Direzione del Partito Radicale Transnazionale. «È assolutamente inaccettabile – ha affermato Cortiana - che chi protesta in modo pubblico e virtuale, come è avvenuto il 15 febbraio con il blocco di diversi siti dell'amministrazione americana, possa essere equiparato a chi riempie le caselle postali di migliaia di messaggi pubblicitari, magari pornografici, e addirittura a chi usa gli strumenti informatici con intenzioni terroristiche». Tanto più che **la decisione di Bruxelles sembra inapplicabile nel nostro Paese, vista la nostra legislazione e la nostra costituzione**. «Un netstrike – spiega il senatore - cioè una contemporanea richiesta di accesso ad un server da parte di migliaia di utenti o l'intasamento di e-mail di una casella da parte degli utenti, è un atto equivalente ad un corteo, quando le strade vengono intasate dai manifestanti, ed è un atto perfettamente legale». E ancora: «La proposta di equiparare questi comportamenti al terrorismo informatico è, a livello comunitario, assolutamente irragionevole e, a livello nazionale, incostituzionale, perché limita la libertà di manifestazione. Ho presentato una interrogazione urgente al ministro Castelli…».

Marco Cappato dimostra, con un esempio, come la direttiva offra una definizione così ampia degli attacchi contro i sistemi informatici, che **teoricamente tutto potrebbe finirci dentro**. «Se faccio una campagna politica contro la pena di morte di Cina – afferma Cappato - e rallento il sito invitando i navigatori Internet a inviare delle email al Parlamento cinese, faccio una cosa diversa dall'introdurmi nel sito di un'industria, rubare i dati delle carte di credito e altre cose del genere. Lo capisce chiunque che le due situazioni non sono per nulla simili. Invece, stando alla nuova direttiva dell'Unione Europea, io posso finire nei guai giudiziari allo stesso mo-

LE NUOVE DIRETTIVE EUROPEE RENDONO ILLEGALE IL NETSTRIKE

do sia nell'uno che nell'altro caso». Che il netstrike sia una pratica non illegale è **persino sostenuto nel "Rapporto sullo stato della sicurezza in Italia", redatto dai servizi segreti nel febbraio 2001** «Sempre più di sovente – si afferma - viene utilizzato l'attacco informatico di tipo Netstrike, che non comporta alcun tipo di reato, poiché si configura come una sorta di corteo telematico, finalizzato a rendere impossibile e comunque difficile la consultazione del sito Internet target».

## >> Le reali intenzioni

A chiarire meglio perché sia "una manifestazione di massa di dissenso civile pienamente legittima e legale" A. Di Corinto e T. Tozzi, gli autori di "Hacktivism. La libertà nelle maglie della rete" (ManifestoLibri, 2002 - www.hackerart.org/storia/hacktivism.htm). «È un'azione assolutamente legale perché metaforicamente è come se un giornale, una radio o una televisione andassero in tilt perché non sono in grado di soddisfare un improvviso aumento di richieste della propria utenza; nessuno mette in atto alcun sistema di boicottaggio ma tutt'insieme, **sommando l'azione legittima e legale di navigare sullo stesso sito alla stessa ora, rendono visibile un'espressione di dissenso**».

Il netstrike, per chi lo attua, è più che altro un atto simbolico. Non ha nessun valore che il sito venga effettivamente bloccato. **Ha valore invece la presa di coscienza e la partecipazione del maggior numero di persone possibile intorno a delle questioni cruciali**. Ha valore soprattutto che la notizia circoli e se ne parli. In pratica il vero netstrike non è rivolto al sito, ma al "circuito dei media che deve essere costretto a presentare la notizia per far sì che se ne discuta".

La direttiva dell'UE ha generato un certo allarmismo anche e soprattutto tra il popolo della rete (se n'è discusso qua e là nei vari forum) ed è apparsa agli occhi di qualcuno come "un disegno preciso teso a criminalizzare le forme di protesta" (www.inventati.org e www.autistici.org).

Anche tra in seno al popolo della rete però si sono aperti dibattiti: se quasi tutti tendono a considerare legittima una mobilitazione contro un sito, fatta da migliaia di persone armate del solo browser, **qualcuno storce il naso nei confronti dell'utilizzo di programmi e script realizzati ad arte per saturare la banda del sito da colpire**. Grazie a questi sistemi, anche pochissime persone che dispongano di una connessione sufficientemente veloce, possono produrre lo stesso effetto. Insomma, un po' come bloccare il traffico cittadino con un TIR disposto di traverso invece che attraverso un corteo con migliaia di partecipanti.

### IL SEQUESTRO DI NESTRIKE.IT

Già nell'agosto del 2001, appena 3 settimane dopo le proteste contro la globalizzazione e il G8, partì dalla magistratura di Genova un provvedimento di sequestro firmato del sostituto procuratore Francesca Nanni di www.netstrike.it. La Polizia Postale immediatamente pose sotto sequestro il server dell'associazione culturale Isole nella Rete (www.ecn.org) che l'ospitava. Poi si scoprì che le motivazioni del provvedimento non avevano nulla a che vedere con il netstrike. Nel mandato, infatti, si citava l'art. 615 quinques del Codice Penale ("Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico") e tutti sanno che il sito allora come oggi (fu infatti quasi subito ripristinato grazie alla solidarietà di tanti; sorsero persino decine di siti mirror, anche in lingua inglese) ha per lo più carattere informativo, insomma non ha nulla a che vedere con la diffusione di virus, cavalli di troia o altri programmi che danneggiano servizi informatici.

## >> Idee fuorilegge?

Se la direttiva miri davvero a criminalizzare le forme di protesta, sarà la storia a dircelo. Di certo equiparare spamming, netstrike e terrorismo informatico rivela l'ignoranza delle istituzioni (così ci piace credere, perché alla "non conoscenza" si può sempre porre rimedio) in materia non solo di "informatica" (informazione + automazione), termine che si riferisce ai processi e alle tecnologie che rendono possibile l'immagazzinamento e l'elaborazione dell'informazione, ma anche e soprattutto della "cultura" che si è sviluppata intorno e grazie ad essa, dove per cultura s'intende qui quel sistema di concezioni espresse in forme simboliche per mezzo delle quali gli uomini comunicano, perpetuano e sviluppano la loro conoscenza ed i loro atteggiamenti verso la vita. In particolare e nel caso specifico, quei principi etici e quegli ideali che sono alla base di molte iniziative, comprese quelle definite in Europa "antagonistiche" dell'Hacktivism di cui il netstrike non è altro che una delle tante forme. Tra gli hacktivist (e quindi anche tra i netstriker) si annoverano non solo hackers e attivisti ma anche scienziati, istituzioni governative, pacifisti, università, scrittori, filosofi, sociologi, politici, insegnanti, intellettuali, artisti e diversi altri soggetti che hanno come principali valori di riferimento, l'uguaglianza, la libertà, la cooperazione, la fratellanza, il rispetto, la lealtà, la pace. Appare chiaro, insomma, che in base alla nuova direttiva dell'UE sarebbero tacciati come "criminali" non solo quei soggetti ma forse persino, indirettamente, quei principi. E in un momento storico in cui si crede nella scelleratezza della guerra per riportare la pace, nell'utilità di un crimine per porre fine ad un altro crimine, il timore è che davvero tutto possa accadere. Di qui la necessità di raccontare e di riflettere!

**DaMe`**
**www.dvara.net/HK**

UNA VECCHIA GLORIA DELL'HACKING, SEMPRE SULLA CRESTA DELL'ONDA

# Eric S. Raymond

29 MAY 1997
MY WISH FOR
PEACE AND HARMONY
AMONG ALL WHO WORK
FOR FREEDOM -
WHETHER IN SOFTWARE
OR ELSEWHERE
ERIC S. RAYMOND

**Uno dei pochi che riesce a comprendere lo spirito di una comunità, e a raccontarlo al resto del mondo in una forma comprensibile.**

Raymond è considerato, e a ragione, il catalizzatore della coscienza sociale e l'addetto alle pubbliche relazioni della comunità hacker e open source. Pare infatti che la sua specialità (oltre a programmare in ambiente Unix come pochi), sia quella di **catturare lo spirito di una comunità, estrarne i concetti fondamentali, e comunicarli a un pubblico più vasto**. Non che gli hacker non sapessero di essere una comunità particolare prima che lui integrasse e diffondesse **il Jargon File** (un dizionario dei termini della cultura hacker, iniziato negli anni '60); solo che prima di lui non erano ben chiari ed espliciti i principi, le relazioni e i valori su cui questa comunità si fondava. Il Jargon file è una lettura consigliatissima. Non si tratta di un semplice e sterile dizionario, ma piuttosto di una enciclopedia della cultura, che **si sofferma spesso sugli aspetti più divertenti della faccenda** (provate a leggervi le definizioni di automagically, pr0n, e real programmers…).

"The most important book about technology today, with implications that go far beyond programming." —Guy Kawasaki

THE CATHEDRAL & THE BAZAAR
MUSINGS ON LINUX AND OPEN SOURCE BY AN ACCIDENTAL REVOLUTIONARY
ERIC S. RAYMOND

## >> La cattedrale e il bazaar

Lo stesso ruolo, più di trenta anni dopo, lo ha svolto con la comunità open source. Il suo libro **"La cattedrale e il bazaar"** ha evidenziato i vantaggi dello sviluppo software in una comunità aperta e non direttamente controllata (il bazaar), rispetto a una struttura gerarchica rigidamente organizzata (la cattedrale). Per dimostrarlo, Eric ha usato il metodo scientifico: lo ha sperimentato su un progetto software che stava conducendo, analizzando le differenze con le dinamiche di sviluppo tradizionale.

Ma Eric è andato ben oltre. **Ha dato al movimento un nome e uno slogan** che potesse essere apprezzato e abbracciato da un pubblico più vasto, e soprattutto dalle grandi aziende del software. Agli inizi, l'unica filosofia celebre nel campo del software libero era quella di Richard Stallman e del progetto GNU. La più radicale e quindi la più temuta dalle aziende, che mai e poi mai avrebbero accettato di avere a che fare con licenze così restrittive. **Stallman era visto come un rivoluzionario che voleva abbattere l'industria del software in generale, e non solo quella del software proprietario.** O meglio: allora, esisteva solo l'industria del software proprietario, e poco altro. E quell'industria era intimidita dall'ambiguità del termine inglese "free", che significa "libero" ma anche "gratuito".
Eric Raymond, insieme ad altri membri della comunità hacker, ha allora creato un nuovo tipo di licenza meno restrittiva, e ha contribuito a dare al concetto un nuovo nome, più accattivante anche per le grandi aziende: **"open source"**.

### LINK SU ERIC RAYMOND

www.catb.org/~esr/
La home page personale di Eric, recentemente spostata dal dominio tuxedo.org.

http://armedndangerous.blogspot.com
Eric ha idee molto radicali, e le esprime con forza. Anche quando sono su argomenti controversi, come la libera circolazione della armi

www.apogeonline.com/openpress/libri/index.html
La cattedrale e il bazaar, prima versione, in italiano.

http://linuxpr.com/releases/3308.html
Nuova versione, in inglese.

http://virgolamobile.50megs.com/hacker-howto-it.html
Come diventare un hacker, in italiano.

CREARE VIDEO CD A PARTIRE DA FILMATI PER COMPUTER

## Stufi di vedere filmati sul monitor del computer? Stareste più comodi sul divano del salotto che sulla sedia della vostra scrivania? Createvi un bel Video CD e infilatelo nel lettore DVD di casa!

Per prima cosa vediamo cos'è il VCD (Video Compact Disc) esso rappresenta **un CD che può contenere audio, video e immagini fisse con sottofondo audio**. Costituisce un formato standard e per questo motivo gli consente di essere **riproducibile dai lettori DVD casalinghi**. Ovviamente un VCD può essere letto anche dalla totalità dei Lettori CD-ROM e DVD-ROM per computer. La qualità di un video CD è pressoché paragonabile a quella di una cassetta VHS (e quindi ben inferiore a quella di un DivX codificato bene).

La compressione video è la MPEG1 mentre il bit rate video è 1150 kbits/sec, la risoluzione è 352x288, la compressione audio MPEG1 layer I, il bit rate audio 224 kbits/sec, la frequenza di campionamento audio 44.1 kHz. Il tutto, praticamente, si traduce nel fatto che **un minuto di video occupa circa 10 Mbyte, e quindi su un VCD si può far stare all'incirca un'ora di filmato**.

Prima di iniziare, una raccomandazione. Se è vero che praticamente ogni lettore DVD da casa è in grado di leggere anche i Video CD, **non tutti accettano di buon grado un CD masterizzato**. Prima di convertire l'intera collezione, conviene quindi fare una prova (anche di pochi minuti) e verificare che il proprio DVD player possa leggere un CD-R.

## >> Come operare

Per poter trasformare il nostro DivX in VCD si possono usare vari metodi e programmi. Noi useremo **TMPGenc** per Windows, che si può scaricare da www.tmpgenc.net.

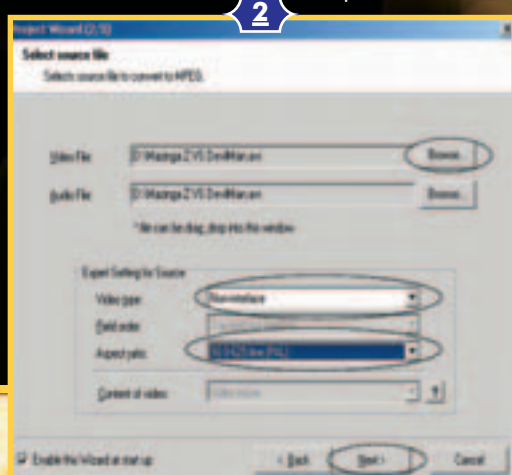
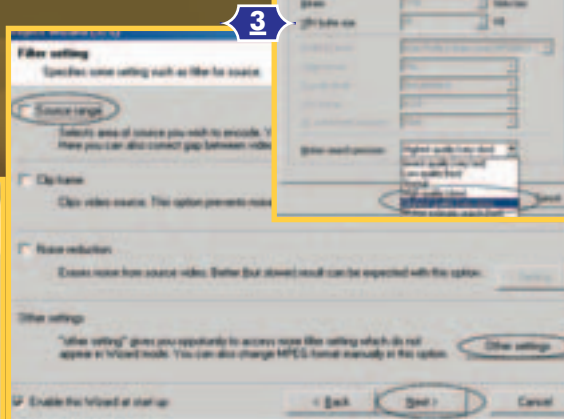
1 La prima cosa da fare è procurarci un filmato, magari ottenuto dalla

# COME TI MASTERIZZO IL DivX

1

nostra precedente copia in DivX di un nostro DVD.

Facciamo partire il programma, ci troveremo di fronte alla schermata del wizard (figura 1) scegliamo sul menù a destra la voce **Video-Cd -> Pal** e facciamo clic su **Next**.

**2** Ci troveremo di fronte alla seconda finestra del wizard (figura 2) che ci chiede di inserire la posizione del file da convertire. Facciamo quindi clic alla voce **Video file** su **Browse...** e scegliamo il nostro filmato da convertire. Una volta fatto ciò, nella sezione in basso scegliamo il tipo di video **Non-Interlace** e come **Aspect ratio** mettiamo **16:9 625 line (PAL)** quindi facciamo un bel clic su Next...

2

3

**3** Nella terza finestra del wizard (figura 3) premiamo su **Other settings**. Ci compare la finestra **MPEG setting** (figura 3b) dove, per ottenere una migliore qualità del formato, dobbiamo scegliere in **Motion search precision** la voce **Highest quality (very slow)**. Ora possiamo fare clic su **Ok** e poi su **Next.**

**4** La quarta finestra (figura 4) ci fa vedere la durata del nostro filmato; nel caso in cui superasse gli 80 minuti (ed è quasi sicuro, perché un normale film della durata di 110 minuti compresso in DivX occupa 700 Mbyte circa, mentre compresso in VCD occupa 1,4 Gbyte), allora dobbiamo tornare

4

indietro nella terza schermata del wizard e selezionare la voce **Source range**.

## LINK UTILI

http://digilander.libero.it/divxdoor1/home.html
www.geocities.com/itadivxgang/
http://sly.thekey.it/
http://digilander.libero.it/divxdoor1/VCD/vcd_guide.html
www.divax.it/guide/vcd.asp

5 Comparirà automaticamente la finestra **Source range** (figura 5) che ci permette di settare l'inizio e la fine del filmato. Posizioniamoci quindi cir-

5

ca a metà del filmato, facciamo clic su **Set end frame** e segniamoci da parte il valore corrispondente nella finestra **End frame**. Proviamo ora a cliccare su **Ok** e poi su **Next** per vedere se ora lo spezzone rientra negli ottanta minuti. Se tutto va bene, facciamo clic su **Next**.

6 Questa è l'ultima finestra (figura 6). Prima di far partire la trasformazione del filmato, nel caso in cui lo stesso non rientra negli 80 minuti, conviene selezionare la voce **Create another project(s) for batch encoding**, fare clic su **Ok** ancora su **Ok**.

7 Ripetere i passi precedenti fino alla terza finestra, quindi nella finestra **Source range** impostare **Start frame** secondo il valore che ci siamo annotati precedentemente e quindi premere Ok e poi due volte **Next**. Dare il segno di spunta a **Start encoding immediately**, premere **Ok** e aspettare che il lavoro sia finito.

6

## >> Masterizzare il risultato

Ora non ci resta che masterizzare il nostro VCD. Per farlo ho utilizzato Nero Burning Rom.

8 Per prima cosa facciamo partire Nero e scegliamo **Video-Cd** (figura 7). Selezioniamo **Crea un CD compatib. Standard** e **Usa applicazione CD-i**.

7

8

9 Andiamo poi alla voce **Menu** (figura 8) e selezioniamo **Attiva menu**. In questa finestra possiamo personalizzare l'aspetto che deve avere il VCD sul televisore. Una volta terminato andiamo su **Iso** e impostiamo **Iso level 2 (max 31 caratteri)**.

10 Infine selezioniamo **Nuovo** e individuiamo quindi il nostro file MPEG attraverso il menù di navigazione di destra (figura 9) e trasciniamolo nel campo

9

vuoto in basso a sinistra. Ora non ci resta che masterizzare il CD e inserirlo nel lettore DVD di casa.

**KoRn**
**issues75@libero.it**

## LA VIA PIU' SEMPLICE

Il procedimento che vi abbiamo spiegato vi sembra troppo complesso? Sappiate che iniziano a vedersi sugli scaffali dei negozi i primi lettori DVD che leggono i formati DivX e Xvid. Qui, ad esempio, il DV-450 Digisette che trovate a 456 euro di listino.

IDENTIFICAZIONE DEL CHIAMANTE, NUMERI RISERVATI E MONITORAGGIO COSTANTE

# TELEFONO ANONIMO

**Anche con un telefono di casa è possibile nascondere il proprio numero quando si chiama qualcun altro, ma non fateci troppo affidamento...**

Da quando ci sono i telefoni cellulari è diventata evidente una cosa che chi ha un minimo di dimestichezza con la tecnologia aveva già ben chiara da tempo: è possibile vedere il numero di chi ti sta chiamando. Questa funzionalità è chiamata "Caller ID" (identificativo del chiamante) o CLI (Calling Line identification). Chi desidera mantenere un po' di riservatezza, può impostare il cellulare per non rivelare questo numero. E sul telefono di casa?

## >> Numeri riservati

La legge sulla privacy ha finalmente consentito anche in Italia di rendere il proprio numero "riservato". Con un'opportuna richiesta a Telecom, **è possibile fare in modo che il proprio numero telefonico non compaia nell'elenco, né sui visori dei cellulari o telefoni fissi abilitati al servizio "Chi è?"**, che appunto corrisponde all'identificazione del chiamante. Chi non vuole prendere misure così drastiche ha ancora una possibilità: il **Blocco Identificativo Chiamante**. Prima di chiamare una persona alla quale non si vuole rivelare il proprio numero, bisogna comporre il codice ***67#** (o **4793** se non si dispone di un telefono a tastiera). In questo caso, il numero rimarrà riservato, ma **solo per quella chiamata.**

## >> Occhio però...

Innanzi tutto, chi riceve telefonate moleste, **può chiedere di visualizzare sul proprio telefono, per un breve periodo, anche i numeri riservati**. Inoltre, il blocco identificativo del chiamante permette di impedire la visualizzazione del numero all'altro capo della linea, ma **Telecom e tutti gli operatori telefonici coinvolti nella chiamata in corso, registrano sicuramente la chiamata in un database**. Ogni tanto nei siti H4x0r più scrausi si leggono tutorial su come rendere anonime le proprie telefonate con i "codici magici" da comporre prima del numero. Ebbene, i "codici magici" sono ben descritti nel sito di Telecom Italia, e **non servono assolutamente a evitare una bella perquisizione** a casa di chi compie qualche scorreria di troppo col telefono o con una connessione a Internet su linea dial-up.

## >> Internet e provider

A proposito di provider, è bene sapere che, siccome è possibile sottoscrivere un abbonamento Free Internet fornendo dati completamente falsi (solitamente basta un normale generatore di codice fiscale, o il saperlo calcolare), l'unico modo che i provider hanno per tutelarsi da un utilizzo fraudolento della propria rete (ed eventualmente per poter comunicare alla polizia l'autore del misfatto), è proprio quello di **registrare il numero telefonico della linea da cui viene effettuata la telefonata** E, nonostante le nostre intenzioni di riservatezza, la legge è dalla loro parte.
Insomma, chi pensa di essere anonimo su Internet solo perché ha registrato il proprio account come un "Mario Rossi" qualunque, **si sbaglia di grosso.**

## PERCHE' RENDERE ANONIMO IL PROPRIO NUMERO?

**In Italia probabilmente è ancora un'esigenza poco sentita, ma negli USA la situazione è diversa. Lì infatti le aziende hanno il diritto di raccogliere i numeri di telefono di chi chiama un loro centralino, e poi possono farne ciò che vogliono. Quindi, se uno chiama un negozio per chiedere un'informazione, il negozio potrebbe immagazzinare quel numero e chiamarci in futuro per proporre offerte e prodotti. Oppure può "venderlo" ai propri fornitori, che lo possono passare ad altri e così via, esattamente come accade con lo spam per posta elettronica.**

# IL TUO MAC

**Credete che basti una password per proteggere i vostri documenti dagli sguardi indiscreti? O pensate che Unix sia una parola magica che garantisce sicurezza, indipendentemente da come si configura il sistema? Meglio che ci ripensate...**

Mac OS X è basato su un cuore Unix e questo, nel bene e nel male, comporta profondi cambiamenti all'aspetto della sicurezza della macchina. Se Se da un lato è possibile difendere maggiormente l'accesso locale o remoto, proteggendolo con password, chi riesca a superare queste difese potrà controllare il computer in modi prima impensabili con un sistema Classic.

## >> Multiutenza, ma non troppo

Mac OS X permette la gestione di più utenti, ognuno dei quali non può accedere alle cartelle degli altri utenti, ma è impostato per effettuare il login automatico dell'utente principale. Per ottenere all'avvio una finestra che richieda la password prima di dare accesso al computer, occorre andare in Preferenze di Sistema, aprire il pannello Account, fare clic su Opzioni Login e poi selezionare l'opzione Nome e password oppure Lista di utenti dalla voce Mostra la finestra di Login come... La prima opzione farà apparire un modulo anonimo, in cui inserire username e password; la seconda invece presenterà una lista di tutti gli utenti registrati, e rimarrà da inserire la sola password. Ovviamente, la prima opzione è quella più sicura, perché un eventuale malintenzionato dovrà indovinare due parametri (nome utente e password) invece che uno solo. In questo pannello abbiamo altre due opzioni. Nascondi i pulsanti Riavvia e Spegni impedirà di effettuare queste operazioni dalla finestra di login (ma, come vedremo più avanti, hanno un'utilità molto dubbia); la seconda invece, dopo tre tentativi falliti di login, visualizzerà un suggerimento utile a ricordare la password (questo suggerimento si può impostare opzionalmente nel pannello Il Mio Account). È ovvio che, se si inserisce un suggerimento troppo evidente (qual è la mia squadra del cuore?), si vanificherà ogni tentativo di rendere sicura la propria macchina.

Qualsiasi amministratore può agire sotto le spoglie di un altro utente qualsiasi, anche root, con il comando sudo.

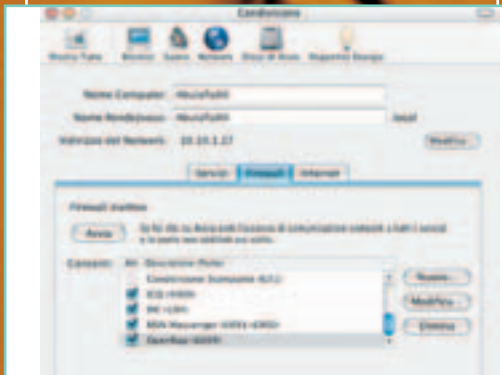
## >> Aggirare il login

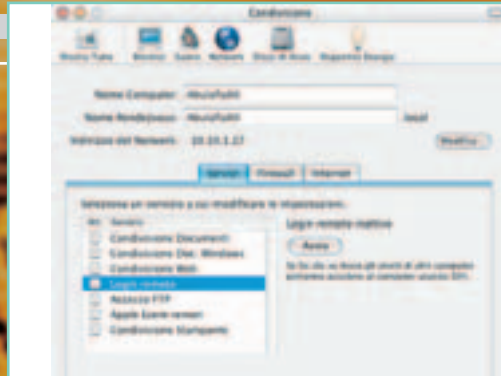
Avendo costruito Mac OS X come sistema personale, e non come un server aziendale, Apple ha preferito dare più importanza al fatto che un utente, per quanto imbranato sia, possa comunque usare il computer, piuttosto che alla creazione di un sistema sicuro al 100%. Per questo, sono state previste due "scappatoie" al sistema di login, che possono essere usate per esempio se si dimentica la propria password. La prima e più semplice scappatoia è la possibilità di cambiare la password usando l'utilità apposita inserita nel CD di sistema (la si seleziona dal menu Applicazione del programma di installazione, , il primo a sinistra, dopo aver riavviato dal CD di sistema).
La seconda "scappatoia" è la modalità utente singolo. In sintesi, premendo Comando+S all'avvio del Mac, ci si ritrova collegati alla console a linea di comando con i privilegi di root (il massimo livello di sicurezza degli utenti Unix) e da lì (conoscendo la sintassi giusta) si può eseguire qualsiasi operazione (le operazioni per fare ciò, così come il modo per impedire questo tipo di accesso, sono descritti in un articolo pubblicato sul n. 5 di HJ: correte a leggervi l'arretrato sul sito, usando le password di pagina 3).

## >> Amministratori e super utenti

Mac OS X contempla due tipi di utente: normale o amministratore. Un amministratore può svolgere alcuni compiti interdetti all'utente normale, come l'installazione di applicazioni particolari o aggiornamenti di sistema, la modifica di alcune impostazioni critiche e così via. Per chi è pratico di altri sistemi Unix, bisogna specificare una cosa: un amministratore non ha esattamente le stesse facoltà dell'utente root. Ancora una volta, Apple ha scelto di creare un ambiente più sicuro anche per gli utenti meno esperti; un utente root potrebbe infatti apportare al sistema delle modifiche che lo renderebbero inutilizzabile.
Queste differenze hanno alcune implicazioni anche nella sicurezza e nella riservatezza dei dati: persino un utente amministratore infatti non può accedere alle cartelle riservate di altri utenti. Detto

# E' SICURO?

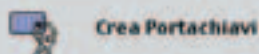
ciò, dobbiamo però precisare subito una cosa: qualsiasi utente amministratore ha la possibilità di diventare temporaneamente un "super utente", semplicemente fornendo la propria password. Un "super utente" ha le stesse facoltà di root, e quindi viene a mancare la riservatezza degli altri utenti a cui accennavamo prima. A differenza di Linux e altri Unix, dove il comando per eseguire un comando come super utente è semplicemente "su comando", su Mac OS X la sintassi da utilizzare è "sudo comando" (Super User do…). Dopo aver inserito il comando, ci verrà richiesta la nostra password di amministratore. Da quel momento, e per un

Il firewall integrato è molto potente, ma l'omonimo pannello permette di configurare solo una ridotta serie delle opzioni disponibili.

certo periodo di tempo, ogni comando impartito verrà interpretato come se fosse eseguito dall'utente root (o da un altro utente specificato nel comando sudo). Ripetiamo un concetto importante: la password richiesta non è quello dell'utente che si vuole impersonare (root o altro) ma la propria.

I servizi che si possono attivare in Mac OS X possono esporre il computer a rischi di sicurezza.

Per sintetizzare quanto detto in questo paragrafo, conviene non assegnare la facoltà di "utente amministratore" a persone alle quali non affidereste le chiavi di casa, della macchina, il PIN del bancomat e le vostre lettere d'amore.

## >> Porte e servizi

Come impostazione predefinita, nessun servizio di condivisione o accesso remoto è abilitato in Mac OS X. Questa è cosa buona e giusta, perché (bisogna ricordarlo?) ogni servizio aperto all'esterno può essere sfruttato per guadagnare accesso incondizionato al computer. I servizi previsti di sistema sono la Condivisione Documenti, su protocollo AppleShare, la Condivisione Documenti Windows (in pratica un server Samba), la Condivisione Web (Apache), Login remoto (telnet con cifratura SSH), Accesso FTP, Apple Event remoti (possibilità di rispondere a messaggi Apple Event lanciati da altre macchine; in pratica, un AppleScript lanciato su un altro Mac può compiere operazioni sulla nostra macchina), e infine Condivisione Stampante. Oltre a ciò, su Mac OS X sono installati (ma disattivati di default) altri programmi che, se attivati, potrebbero mettere a rischio la sicurezza del sistema (uno su tutti, Sendmail). Prima di attivarli, conviene informarsi bene sui possibili rischi. Il pannello Condivisione (dal quale si possono attivare tutti i servizi citati in precedenza) contiene anche una sezione Firewall, che attiva il servizio firewall di sistema (ipfw) e permette alcune spartane configurazioni. Normalmente il firewall è disattivato; se lo si attiva, bloccherà ogni comunicazione in ingresso tranne quelle specificate nella colonna "Consenti". In questa colonna verranno automaticamente abilitate le porte relative ai servizi di sistema contemplati nella sezione Servizi del pannello Condivisione, ma ogni altro programma aggiuntivo che abbia bisogno di connessioni in ingresso deve essere abilitato manualmente, creando una nuova impostazione.

Le impostazioni relative agli account utente.

## Il portachiavi

Nella cartella Applicazioni/Utilities c'è un'interessante programmino chiamato Accesso Portachiavi. In Mac OS X, un "portachiavi" è un file cifrato che racchiude password e chiavi di accesso ad applicazioni o servizi di vario tipo. Per esempio, si possono memorizzare nel portachiavi le password di volumi di rete, di servizi protetti da autenticazione, e persino quelle per accedere a una pagina Web protetta (se il browser supporta questa funzionalità). Quando sarà necessario inserire la password in questione, l'applicazione interrogherà Accesso Portachiavi, che gliela fornirà in modo trasparente o esplicito, a seconda delle impostazioni prescelte. A riguardo, ci sono molti aspetti di cui parlare (tra cui le modalità per forzare o decifrare il portachiavi), e lo faremo in un altro articolo. Per ora ci interessa focalizzare l'attenzione su una cosa. Il Portachiavi stesso è ovviamente protetto da una password. Se questa password non è abbastanza robusta (lunga e composta da lettere e numeri senza significato), tutte le password contenute all'interno, anche quelle robuste, diventeranno immediatamente deboli come la password del Portachiavi. In sintesi: la robustezza di ogni password è determinata dalla complessità della chiave del Portachiavi.

20_22_hj23_map 8-04-2003 10:31 Pagina 20



COME NMAP VIENE USATO PER TECNICHE DI ATTACCO

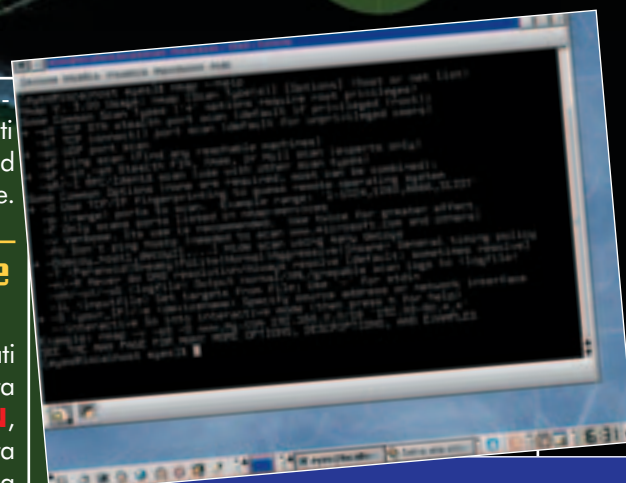
# Uno scanner dalle potenzialità "NASCOSTE"

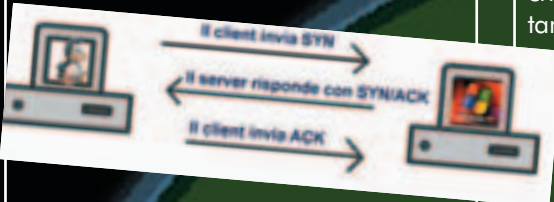
**La scansione delle porte è un passaggio obbligato per studiare la sicurezza di un Sistema Informatico. Analizziamo Nmap, uno degli strumenti più completi nel suo genere.**

Nmap è uno strumento tanto versatile quanto potente che presenta come punto negativo soltanto una relativa difficoltà di utilizzo. Lanciando il comando di help dalla console **si può rimanere un po' disorientati davanti alle numerose opzioni** che sono state implementate in questo strumento dal suo sviluppatore, Fyodor. Nmap, infatti, non offre soltanto le funzionalità di base di un qualsiasi port scanner **ma comprende anche altre tecniche di scansione che ci forniscono informazioni più dettagliate sull'host o sulla rete analizzati**. Prima di vedere perché NMap è considerato uno strumento potente dagli "addetti ai lavori", è necessario analizzare le diverse tecniche di scansione. Uno dei pionieri nell'implementazione di queste tecniche di scansione è Fyodor, che ne ha implementate un buon numero anche nel suo software. Il port scanning (o scansione delle porte ) consiste nella connessione alle porte TCP e UDP dell'obiettivo analizzato. Esistono differenti modalità di scansione. Andiamo ad analizzare in dettaglio alcune di queste.

## >> Le tecniche di scansione

**Tcp connect scan**: Vengono inviati dei pacchetti ad una determinata porta secondo una procedura a tre fasi, **SYN**, **SYN/ACK** e **ACK** (figura 2). Questa tecnica è la più semplice da portare a termine ma anche quella più facile da intercettare. Se non specifichiamo nessun parametro dalla riga di comando, Nmap porterà a termine questo tipo di scansione perché **questa è la tecnica impostata di default**.

**Tcp syn scan**: con questa tecnica di scansione non viene realizzata una connessione completa. Infatti viene inviato un pacchetto SYN alla porta del nostro obiettivo e si attende una risposta. In base al pacchetto che riceveremo, possiamo capire se la porta è in stato di listening o meno. Se infatti la risposta sarà SYN/ACK la porta è in ascolto, mentre se riceviamo un pacchetto RST/ACK la porta non è in ascolto. Il sistema dell'attacker risponderà con RST/ACK, in modo che la connessione non venga mai completata. Que-

Lanciando il comando nmap —h sarà visualizzato l'elenco delle opzioni che corrispondono alle differenti tecniche di scansione.

sta tecnica **consente all'attaccante di muoversi in modo più discreto, evitando di lasciare la sua "firma" nel file di log**. L'opzione da digitare per effettuare questa scansione è **–sS**.

Lo schema semplificato in cui vedete come avviene la connessione TCP in tre fasi.

**Tcp Fin scan**: utilizzando questa tecnica invieremo un pacchetto di tipo FIN sulla porta dell'obiettivo. Il sistema sottoposto a scansione dovrebbe rispondere con RST per tutte le porte che non sono in ascolto. Di solito questa tecnica **funziona in ambiente Unix**. In Nmap questa scansione viene implementata con l'opzione **–sF**.

**Tcp windows scan**: analizzando la dimensione della finestra TCP, con questa tecnica di scansione è possibile individuare **sia le porte in ascolto, sia quelle filtrate in alcuni sistemi**, come in FreeBSD.

**Tcp rpc scan**: questa tecnica viene utilizzata per riconoscere e identificare le porte RPC (acronimo che sta per Remote Procedure Call) insieme al loro numero di versione. In Nmap possiamo realizzare una scansione di questo tipo con l'opzione **–sR**.

**Udp scan**: questa tecnica prevede l'invio di un pacchetto UDP sulla porta del nostro obiettivo. Se questo risponde con un messaggio di errore ci indica che la porta è chiusa. Ovviamente se non riceveremo tale messaggio possiamo facilmente intuire che la porta da noi analizzata sia aperta. Questa tecnica viene eseguita sfruttando il protocollo UDP, quindi il processo di scansione sarà estremamente lento ed inoltre non ci garantisce risultati affidabili. Nmap supporta anche la scansione UDP, inserendo come parametro l'opzione –sU.

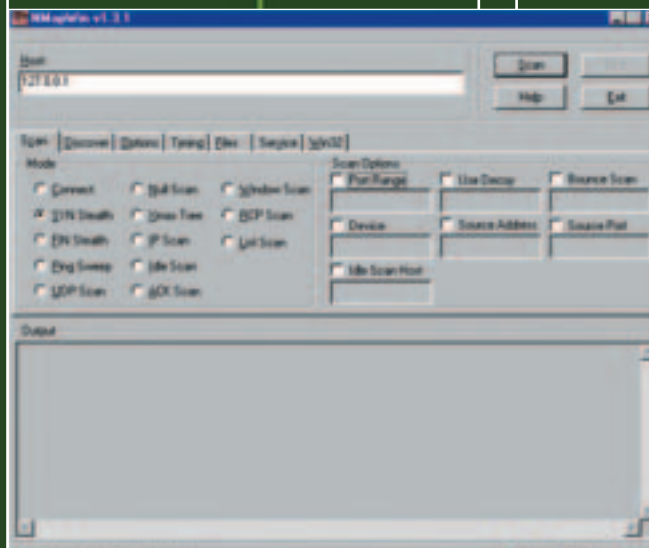
## >> Un po' di pratica

Oltre a queste tecniche esistono altri tipi di scansione supportati da Nmap, che senza dubbio lo differenziano dai tanti software simili che si trovano sulla rete. Dopo avere installato il port scanner (alcune distro Linux già lo includono), digitate il comando:

```
nmap - -help
```

A questo punto (figura 1) vedrete comparire una serie di comandi che vi permetteranno di utilizzare le più svariate tecniche di scansione. È possibile effettuare la scansione TCP con connessione semplicemente digitando

```
nmap 127.0.0.1
```

Infatti, questa è la tecnica di scansione di default e quindi è possibile omettere l'opzione relativa a questo tipo di scansione (ovviamente, al posto di 127.0.0.1 ci andrà l'indirizzo dell'host

Ecco NmapWin, la versione di Nmap per Windows che si presenta attraverso una comoda interfaccia grafica.

**-oN** invece sarà possibile salvare il risultato delle nostre scansioni in un file da noi specificato, mentre inserendo come parametro **–oM** l'output del programma sarà inserito in un file di testo formattato, cioè i campi saranno separati da caratteri di tabulazione. Quest'ultimo comando può essere di grande aiuto quando si effettuano scansioni di un certo range di IP, per cui la quantità di dati andrà formattata in modo da essere leggibile più chiaramente. Vediamo quindi come possiamo utilizzare questo parametro dalla riga di comando:

```
nmap 127.0.0.1 / 24
-oM risultati_scan.txt
```

In questo caso il risultato della scansione del range IP da 127.0.0.1 a 127.0.0.24 sarà salvato nel file di testo, in modo da poter essere consultato anche dopo avere terminato le ricerche.

## >> Ingannare i firewall

Se inoltre non si riuscisse a effettuare un port scanning in una macchina perché questa utilizza come firewall un dispositivo di filtro dei pacchetti, **si possono tranquillamente spezzare i pacchetti in più frammenti**. L'opzione che ci permette di utilizzare tale tecnica è il parametro **–f**. In pratica, questa opzione suddivide l'intestazione TCP su più pacchetti, quindi un sistema IDS (Intrusion Detection System, ne abbiamo parlato nel numero scorso…) **avrà difficoltà a riconoscere la scansione**.

Questa opzione tuttavia non ci offre un elevata discrezione. Infatti i moderni firewall accodano i frammenti di pacchetti IP prima di esaminarli. Anche in questo caso, però, Nmap fornisce opportunità di "camuffamento" senza dubbio più discrete rispetto a quella precedente. L'opzione che ci permette di l'host obiettivo della nostra scansione è **–D** (decoy). Questo termine tradotto letteralmente vuol dire "inganno" ed effettivamente rispecchia benissimo la tipologia di scansione che viene usata specificando questa opzione dalla riga di comando. Utilizzando questa tecnica, infatti, verranno lanciate **una**

20_22_hj23_map 8-04-2003 10:31 Pagina 22



In questa immagine, prelevata dal sito ufficiale di Nmap (www.insecure.org ), possiamo ammirare il nostro portscanner preferito al lavoro.

**serie di scansioni fasulle insieme a quella vera**. In questo modo il sistema che stiamo analizzando risponderà sia agli indirizzi contraffatti sia a quello vero.
La difficoltà dell'host target sarà quindi quella di risalire a tutte le scansione e di **riuscire a individuare quella vera tra tutte quelle false**.
Bisogna fare attenzione a che gli indirizzi fasulli siano effettivamente attivi, altrimenti il sistema obiettivo si troverà sommerso da pacchetti SYN e questo potrebbe causare un DoS (Denial of Service).

Eccovi un esempio dell'utilizzo di questa tecnica:

```
nmap 192.124.1. 1
-D 10.1.1.1
```

Questa opzione è assente nella maggior parte dei port scanner e rende Nmap uno strumento davvero unico nel suo genere, tanto da farlo spesso catalogare come tool malizioso invece che come legittimo strumento di analisi di una rete.

## >> Raccolta di informazioni

Un'altra opzione interessante di Nmap è quella che ci permette di **individuare il sistema operativo che utilizza l'host che stiamo analizzando**. Sfruttando alcune caratteristiche proprie dei pacchetti ricevuti, come per esempio la dimensione della finestra iniziale TCP, Nmap riesce ad individuare con precisione il sistema operativo utilizzando l'opzione **-O**. Se nella macchina obiettivo è aperta soltanto la porta 80 possiamo risalire con alta precisione al tipo di sistema operativo montato su quella macchina proprio utilizzando tale porta. Eccovi un esempio che chiarisce tutto:

```
nmap -p80 -O 192.124.1.1
```

Attraverso l'opzione **-p** possiamo specificare la porta da andare ad analizzare e con l'opzione **-O** risaliamo invece al sistema operativo.

## >> Raccomandazioni finali

È bene ricordare ai più "distratti" che le tecniche di port scanning sono al limite della legalità (tuttora la questione è controversa). Infatti, se in pochi avrebbero da obiettare se qualcuno effettuasse la scansione delle porte di una classe ristretta di indirizzi IP e su porte che corrispondono ai servizi più comuni (come ad esempio la 25, 110, 80…), **è davvero difficile giustificare legalmente qualcuno che effettua scansioni a tappeto su un ampio range di IP**, magari intento a individuare **proprio le porte utilizzate da alcuni trojan**.
Ovviamente, **l'utilizzo di nmap per verificare e analizzare la propria macchina o la propria rete è perfettamente lecito**. Per esempio, potrebbe essere usato sul proprio PC per vedere se è veramente sicura o per verificare di avere configurato in modo ottimale il vostro nuovo firewall. Oppure, un amministratore di rete potrebbe effettuare una scansione delle macchine alla ricerca di porte utilizzate dai trojan, e ripulire la macchina in questione.

**Antonino Benfante**

## E c'è anche nmap per Windows

Ovviamente coloro che usano il sistema operativo di mamma Micro$oft non devono preoccuparsi, perché **è stata sviluppata una versione di questo software anche per la loro piattaforma**, e che utilizza una comoda interfaccia grafica. Tutte le tecniche appena descritte quindi potranno essere utilizzate semplicemente spuntando con un clic le relative voci. L'utilizzo di un'interfaccia grafica però non sempre porta dei vantaggi. Infatti **utilizzando la versione Nmap a riga di comando è possibile realizzare degli script in modo da automatizzare una serie di comandi**, mentre l'interfaccia grafica complica un po' tutto. A parte questo, consiglio di utilizzare Nmap da riga di comando quando magari si è già un po' più smaliziati.

Trovate nmap per Linux e Windows sul CD di Hackers Magazine n. 6

23_25_hj23_prox 8-04-2003 10:33 Pagina 23



COME USARE PROXY, SOCKS E WINGATE PER ANONIMIZZARE UNA CONNESSIONE

# NAVIGARE ANONIMI!

**In tanti vi chiedete (e ci chiedete): "come faccio a essere anonimo in Rete?" La risposta in realtà è semplicissima...**

1 I Proxy Server come dice il nome (in inglese proxy significa 'procuratore') è come una sorta di procuratore digitale che si occupa di trovare per nostro conto delle informazioni in rete utilizzando i classici protocolli (FTP, http eccetera). Un web proxy ad esempio riceve la richiesta di un URL da parte del client, verifica se non possiede già nella sua memoria cache il contenuto di quell'URL, altrimenti inoltra la richiesta al server destinazione per conto del client restituendo poi al client stesso il risultato della sua richiesta. Naturalmente in questo caso nel log del server web di destinazione viene registrato l'IP del proxy e non quello del client (se non avete chiaro cosa sia un Log, leggetevi l'articolo a riguardo in questo stesso numero). I proxy server quindi svolgono due funzioni:

Riducono notevolmente il traffico di rete. Pensate infatti al traffico web di un grosso provider: è probabile che vi siano dei siti più frequentati (motori di ricerca o grandi portali) i quali, risiedendo direttamente nella cache del proxy, evitano che la linea che collega il provider ad Internet venga intasata sempre dalle medesime richieste.

Protegge l'utente nascondendo il suo IP da occhi indiscreti.

Normalmente un proxy server ben configura to dovrebbe consentire l'accesso soltanto a un certo numero limitato di utenti. Poniamo il caso di avere una rete locale che accede ad internet attraverso un web proxy, è ovvio che l'accesso al proxy dovrebbe essere limitato agli utenti provenienti dalla rete interna, evitando quindi di fornire il servizio agli esterni. Questo non sempre avviene per cui è possibile trovare in rete proxy "pubblici" o per scelta o per errata configurazione.

Detto questo, come è possibile trovare un proxy pubblico?

Impostazione di un proxy generale in Internet Explorer.

## >> Proxy pubblici o aperti

La fonte principale sono i motori di ricerca; inserendo parole chiave come proxy list, anonymity si possono trovare svariati siti che a volte contengono liste di migliaia di proxy. A questo proposito ve ne segnalo due:

http://proxyblind.port5.com/
www.multiproxy.org

Nel primo sito troverete una lista di oltre 3000 proxy. Naturalmente non tutti, anzi pochi di questi, risultano attivi (cioè rispondono alle richieste) ed ancora meno sono quelli funzionanti, cioè pubblici (alcuni infatti chiedono la password di accesso al proxy). Per verificare quali sono utilizzabili dovete provarli uno per uno... Naturalmente potete anche scegliere di far fare

COME USARE PROXY, SOCKS E WINGATE PER ANONIMIZZARE UNA CONNESSIONE

Facendo clic su Avanzate nella finestra di Impostazioni rete locale di IE, si possono specificare proxy diversi per i vari protocolli.

tutto il lavoro a un programma. È ciò che fa Multiproxy, un utilissimo tool che trovate nel secondo link che vi ho fornito. Per maggiori dettagli sulla sua installazione e il funzionamento, vi rimando a un articolo pubblicato sul n.7 di HJ, che potete trovare in formato Pdf nella Secret Zone del sito (potete accedere alla Secret Zone con le password pubblicate a pagina 3).
Un altro metodo per la ricerca dei proxy può essere uno scanning delle porte su un certo range di ip. Per far questo un qualunque port scanner va bene. Questo metodo naturalmente è un po' più laborioso però vi consente di trovare proxy poco noti e quindi più longevi. Attenzione però: effettuare una scansione su un range di IP elevato potrebbe essere scambiato per un tentativo di attacco (o quanto meno una fase preliminare di attacco). Non è una pratica consigliabile.

## >> Anonimi ma non troppo

Appoggiarsi ai proxy permette, quindi, di non lasciare il nostro ip sul server di destinazione, ma non ci garantisce l'anonimato al 100%, perché è molto facile che il proxy pubblico attraverso cui stiamo passando registri le attività e quindi il nostro ip. Naturalmente tutto dipende dalle politiche adottate dall'amministratore di sistema: vi possono essere proxy che non registrano i log o proxy che li eliminano il giorno dopo.
Per utilizzare i proxy trovati, dovete configurare il vostro browser (nel caso dei web proxy) affinché inoltri le richieste verso il proxy stesso. Nel caso ad esempio di Internet Explorer è sufficiente andare in Strumenti->Opzioni Internet->Impostazioni LAN. A questo punto, selezionando l'opzione server proxy potete inserire l'IP valido trovato con la relativa porta di utilizzo (per quanto riguarda i web proxy le porte più comuni sono la 8080, la 80 e la 3128) (figura 1). Non mi soffermo molto sulla configurazione di altri browser o applicativi client (es. FTP, IRC eccetera) dal momento che ci sono moltissimi applicativi di vario tipo che supportano i proxy. È sufficiente consultare caso per caso la documentazione online del programma che ci interessa.

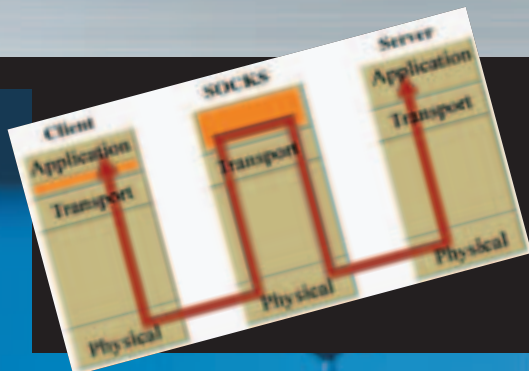
## >> Concatenazione dei proxy

Argomento invece più interessante è la concatenazione dei server proxy. Vi sarà sicuramente capitato di vedere in parecchi film di spionaggio l'hacker di turno che fa rimbalzare il proprio segnale attraverso i computer di mezzo mondo prima di giungere a destinazione. Questo è ciò che può essere fatto con la concatenazione.
Il concetto che sta alla base della concatenazione è abbastanza intuitivo: se posso utilizzare un server proxy inviandogli una richiesta ad esempio di una pagina web, il proxy a sua volta può inviarla al server di destinazione ma può anche indirizzarla ad un altro server proxy e così via, in modo che il log del server di destinazione registrerà soltanto l'IP dell'ultimo proxy e sarà molto difficile, se non impossibile, risalire al mio ip, poiché dovrebbero essere interrogati tutti i proxy intermedi e non è detto che ciò sia possibile, soprattutto se si trovano in paesi diversi.
Tradurre in pratica questo concetto è più facile a farsi che a dirsi: supponiamo di voler raggiungere il sito www.acme.com attraverso una catena di proxy.

Lavorando a un livello diverso dai proxy normali, un Socks proxy può funzionare con applicazioni e protocolli diversi in modo trasparente.

Supponiamo inoltre di conoscere gli ip di 3 proxy che si chiamano rispettivamente: proxy1.com, proxy2.com, proxy3.com (possono essere anche di più). È sufficiente aprire il nostro browser ed inserire l'indirizzo di Acme in questo modo:

http://proxy1.com:80/http://proxy2.com:8080/http://proxy3:3128/http://www.acme.com.

23_25_hj23_prox 8-04-2003 10:33 Pagina 25

Il funzionamento dei Socks Proxy prevede l'utilizzo di un Socks server e un Socks client.

Ho ipotizzato che le porte attive dei tre proxy fossero rispettivamente 80, 8080, 3128. Se non vi va di scrivere indirizzi così lunghi, potete inserire la catena di proxy direttamente nelle impostazioni del browser, però non senza una piccola modifica nella sintassi. Utilizzando Internet Explorer dovete richiamare la finestra su cui è possibile inserire l'IP del proxy come abbiamo visto prima, e digitare nell'indirizzo la seguente stringa:

```
ip_del_proxy1:80
ip_del_proxy2:8080
ip_del_proxy3
```

La porta del terzo proxy (3128) va inserita nello spazio dedicato alla porta. Fatto questo, il browser per ogni indirizzo richiesto invierà la richiesta al primo proxy, il primo al secondo e così via. Detto questo possiamo passare ai socks.

## >> Socks

Il socks a differenza dei proxy è un vero e proprio protocollo creato da David Koblas e poi perfezionato da Ying-Da Lee della Nec per far sì che, in una rete protetta da firewall, i computer interni siano in grado di uscire attraverso il firewall stesso stabilendo delle connessioni all'esterno. La procedura è questa: il client si connette al servizio socks del firewall, generalmente sulla porta 1080, e quest'ultimo si occupa di fare le veci del client nei confronti dell'application server che si vuole raggiungere. Per far questo è necessario un socks proxy server in cui il socks è implementato al livello di application layer e un socks client in cui il socks opera tra l'application layer ed il transport layer (figura 4). Esistono due modelli socks: la versione 4 e la 5. In quest'ultima sono state aggiunte le procedure di autenticazione al socks server, assenti nella versione 4. Se volete approfondire il funzionamento di questo protocollo vi consiglio il seguente indirizzo: www.socks.permeo.com. Qui troverete i documenti originali (purtroppo in inglese!) di Ying-Da Lee in cui descrive brevemente le funzioni della sua creatura. Anche in questo caso come per i proxy è possibile trovare online dei socks che accettino connessioni anche da utenti "esterni". I metodi di ricerca sono gli stessi che abbiamo visto per i proxy ossia: attraverso i motori

Concatenando svariati server Proxy, si può far rimbalzare la connessione ai quattro angoli della terra, rendendola più difficile da rintracciare.

di ricerca (a tal proposito vi indico una lista di socks per cominciare: http://proxyblind.port5.com/listsocks.shtml). Per trovarli, e soprattutto per testarli, è disponibile in rete un'utility chiamata Socks Proxy Finder.
L'utilizzo dei socks trovati è molto semplice poiché, come per i proxy, vi sono un gran numero di applicazioni client che prevede la possibilità di utilizzarli. Su Internet Explorer ad esempio basta andare sulle impostazioni avanzate della finestra di inserimento proxy che abbiamo visto prima (figura 2). Come esempio prendiamo mIRC. Nella cartella firewall del mIRC setup è possibile indicare il socks attraverso il quale connettersi al proprio server IRC. Basta selezionare il tipo di socks e digitare l'IP e la porta. È inoltre possibile utilizzare il socks anche per le connessioni dirette (DCC) tra utenti (figura 3).

## >> Wingate

Concludiamo questo articolo con un breve sguardo su Wingate. Wingate è un proxy server/firewall per Windows. La sua funzione principale è quella di condividere la connessione ad internet tra più computer di una rete locale senza bisogno di un router. Wingate è multiprotocollo quindi è in grado di fare da web-proxy, da ftp-proxy eccetera. Quello che però ci interessa in quest'articolo è il telnet-proxy. Infatti in caso di errata configurazione dei criteri di sicurezza di Wingate, oppure perché qualche simpatico amico vuole fornirci questo servizio in rete, è possibile usarlo per anonimizzarsi via telnet. Il servizio telnet-proxy opera sulla porta 23 (quella standard del telnet) e per utilizzarlo è sufficiente con un qualunque client telnet collegarsi all'IP della macchina con Wingate. Una volta collegati dovreste ricevere il seguente prompt

```
Wingate>
```

A questo punto avete due possibilità: potete inserire l'IP o il nome dominio del vostro target in questo modo:

```
Wingate> ipdestinazione 23
```

oppure potete inserire l'IP di un altro wingate creando così una concatenazione di telnet-proxy:

```
Wingate> ipsecondowingate 23
```

Il vantaggio principale dei wingate è che non registrano gli accessi in file di log. Detto questo, vi invito ad utilizzare le informazioni contenute in questo articolo esclusivamente per la protezione della vostra privacy.

**Roberto "dec0der" Enea**
**enea@hackerjournal.it**

**Ogni operazione che compiamo in rete viene registrata in file di log. Come uno zelante portinaio, registra ogni cosa che facciamo.**

In generale con il termine "log" si indica l'insieme di **tutte le operazioni registrate da un server o un software**: sono log i dati di accesso a un sito Web, lo sono gli errori e le operazioni compiute da un software e registrate in un file dal programma stesso, lo sono i dati immessi tramite la tastiera e registrati da un Keylogger. Per quanto riguarda i log presenti sul proprio computer, questi vengono creati dai vari software e dal sistema operativo stesso per tener conto delle operazioni effettuate e degli errori riscontrati. Venendo ai log che operano in rete, ad esempio quelli di un server, il discorso si fa più complicato ma la morale di fondo è che **quando si fa qualcosa in rete, questa viene registrata e lascia quindi una traccia ben riconducibile al nostro computer**. Perciò prima di compiere azioni illegali sappiate che rimane sempre un segno del vostro passaggio; il log in questo caso agisce come una telecamera di sicurezza che registra tutto quello che succede ed è pronto a testimoniare che voi eravate lì a quell'ora e stavate commettendo un reato. Pensate che semplicemente collegandosi ad un sito Web ci sono in ballo:

- il log del server Web (che registra l'IP con cui risalire al provider)
- il log di accesso del provider (in grado di stabilire che ad una tale ora quell'IP era collegato ad un determinato account)
- il database delle chiamate Telecom (dai cui tabulati si può sapere che una determinata linea modem è stata contattata ad una certa ora dal nostro numero di telefono)

In questo caso la sfida del pirata è quella di aggirare i log cancellando le proprie tracce o nascondendo la propria identità; in alcuni casi **l'archivio di log può essere utilizzato come prova durante il processo** all'intruso.

## >> Errori e statistiche

Naturalmente questo non è l'unico compito di questi piccoli ma preziosi file: il log di un software serve a registrare tutti gli errori riscontrati durante le normali operazioni con precisi riferimenti alle cause per **permettere all'utente di correggere il problema ed evitare il ripetersi di tali errori**. Oltre che alla sicurezza e al controllo, il log di server Web è finalizzato anche a tener traccia dell'andamento di un sito Web, del comportamento dei visitatori e delle loro preferenze al fine di migliorare il servizio.
Tecnicamente i log sono semplici file, da visualizzare con qualunque editor di testo, formati da righe chiamate "hit" (accesso) contenenti numerose informazioni; parlando del log di un server Web, una riga potrebbe apparire come:

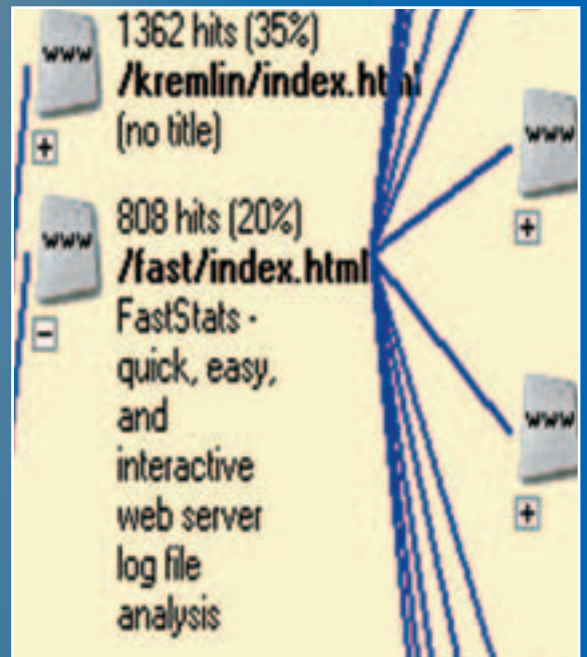
```
2003-03-03 11:13:04
65.113.145.115 - W3SVC104
NL01 62.2.53.11 80 GET
/index.html - 404 2 3536
273 10 HTTP/1.1
Mozilla/4.0+compatible+ZyB/
1.0+(ZyB@WIS.com;+
http://www.crashdown.too.it
) - -
```

In un log ogni riga si riferisce ad una specifica richiesta dell'utente al server per qualunque oggetto necessario al caricamento della pagina come le immagini, i download o

26_28_hj23_log 8-04-2003 10:37 Pagina 27

altri file che saranno registrati singolarmente in altre righe generate nel log dal server.

## >> Privacy a rischio

Come per ogni mezzo di controllo e sicurezza in rete, c'è anche un lato negativo: il log può trasformarsi in una **fonte di informazioni riservate sugli utenti** che visitano un sito Web. Il problema non esisterebbe se questi dati fossero trattati semplicemente a scopo statistico per migliorare e accrescere un sito Web, ma **spesso queste preziose informazioni vengono utilizzate in modo illecito**, quasi sempre per l'invio di messaggi pubblicitari privati agli utenti che si vedono inondate le caselle di posta da E-Mail che promettono facili guadagni e belle ragazze. Oppure per **inviare banner mirati alle proprie preferenze** (ne abbiamo parlato sul numero scorso, nell'articolo relativo ai Cookies). Non c'è un modo per evitare questa tracciatura durante la normale navigazione se non quella di affidarsi a siti che offrono una minima protezione ai dati sensibili. Nel caso questa protezione non basti, ci si può affidare a specifici programmi in rete o proxy che nascondono la nostra identità offrendoci la possibilità di navigare in modo anonimo (ne parliamo più avanti, in questo stesso numero).

## >> Gli analizzatori

Vista l'importanza e il continuo ricorso ai log durante qualunque attività in rete, è semplice capire quindi che, **soprattutto con volumi di traffico elevati, è impossibile interpretare i dati grezzi manualmente.** È dunque necessario affidarsi ai software specifici creati per l'analisi attenta dei log. Per quanto riguarda i log generati dai software o dal sistema operativo, non c'è

bisogno di un programma che li analizzi perché sono di immediata interpretazione e servono solo in caso di errori. Per i log creati durante la navigazione, per

1362 hits (35%)
/kremlin/index.html
(no title)
808 hits (20%)
/fast/index.html
FastStats - quick, easy, and interactive web server log file analysis

esempio quelli di programmi per chattare come mIRC, è possibile analizzarli con software specifici ma in genere non è necessario, in quanto sono di facile lettura e riportano le conversazioni avute durante la sessione di chat. Ben più importanti sono **i software per l'analisi dei log di un server Web** che sono in grado di generare statistiche di ogni tipo sui visitatori.

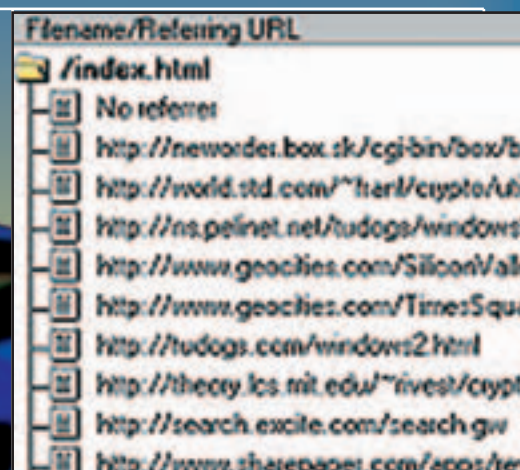
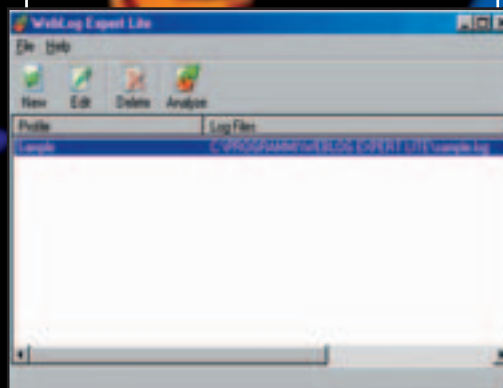
Uno dei migliori programmi per l'analisi dei log di un server Web è WebLog Expert Lite, arrivato ormai alla versione 1.51 e in grado di operare su tutte le versioni di Windows. **WebLog Expert Lite permette di estrarre dal file di log di un sito preziose informazioni sugli utenti e una serie di dati statistici:**

- riassunto generale sul numero di pagine viste, totale visitatori, banda totale e relative medie per giorno e visitatore;
- statistiche dei giorni e delle ore precedenti;
- accessi per pagina, file, immagini, directory, e le pagine di entrata;
- host dei visitatori;
- motori di ricerca più efficienti e parole chiave usate;
- tipo di browser e sistema operativo utilizzato dai visitatori;
- tipi di errori riscontrati nelle pagine, ad esempio il numero di pagine non trovate.

26_28_hj23_log 8-04-2003 10:37 Pagina 28



COS'È UN LOG E COME SI LEGGONO I CAMPI DI UN LOG DI ACCESSO WEB

In pratica il programma legge il file di log e crea delle pagine HTML con i dati statistici sopra descritti. WebLog Expert Lite può essere scaricato gratuitamente al sito www.Weblogexpert.com.
Un altro dei più efficienti software per l'analisi attenta e scrupolosa dei log di un sito Web è **Advanced Log Analyzer**. Il programma capace di operare su tutte le versioni di Windows è in grado di riportare **un'enorme quantità di statistiche differenti** come i referrer più efficienti, i download al giorno, gli host e altri dati sui visitatori ecc. Il software potrebbe essere usato anche come semplice contatore di accessi o dell'attività del sito ma è allo stesso tempo **capace di effettuare un'analisi più approfondita e fornire specifiche informazioni su ogni visitatore**. Facile da configurare e usare, Advanced Log Analyzer assicura la massima precisione nel tracciare e gestire profili generali, che si traducono direttamente in un miglioramento del sito Web ed un conseguente aumento delle visite.
Altro programma utilissimo nell'analisi dei log di un sito Web è **Surfstats Log Analyzer** che provvede a creare le statistiche di accesso dei visitatori in pagine html e grafici. Il programma è anche in grado di **rilevare gli errori nelle pagine Web e i vari aggiornamenti del sito stesso**, i tipi di browser più usati e le pagine più visitate; particolarmente adatto ai siti di utenti privati piuttosto che a quelli grandi aziende.
Le versioni shareware di entrambi questi programmi possono essere scaricare all'indirizzo http://download.com.com/3120-20-0.html?qt=log&tg=dl-20 in cui figurano i download per software in grado di studiare e classificare ogni tipo di log.

## UN LOG VISTO DA VICINO

```
 1               2 3               4                   5                          6   7
rm258.fav.usu.edu - -   [31/May/1995:09:03:23 +0600] "GET /NEI.html HTTP/1.0" 302 396
```

**I CAMPI PRESENTI IN UNA RIGA DI UN LOG COMUNE SONO:**

1 - **Identificazione dell'host che richiede un file dal server Web.**

2 - **Identificazione dell'utente in base all'username secondo la RFC 931. Questo campo viene usato molto raramente, per cui spesso è rappresentato da un trattino (come tutti i campi omessi).**

3 - **Autenticazione dell'utente, usato per le aree protette del sito. A meno che il sito non abbia un'area protetta da password, in questo punto comparirà un trattino.**

4 - **Time Stamp: la data e l'ora in cui qualcuno ha richiesto un file sul server.**

5 - **Richiesta Http: può servire a determinare tre cose: il metodo usato dal client remoto per richiedere l'informazione, il file richiesto e la versione HTTP del client.**

6 - **Il codice di stato indica se il file è stato inviato correttamente, se non è stato trovato, se è stata usata una copia della cache e molto altro.**

7 - **Volume di dati trasferiti. Indica il numero di byte trasferiti al client in risposta all'operazione.**
**Nella sua versione estesa, il log di accesso di un server Web può registrare anche il tipo di browser e di computer utilizzati e, il sito di provenienza.**

# L'ultimo degli Apache

**Volete installare il Web server Apache sulla vostra Linux box? Oppure rimuovere e aggiornare una versione precedente? Ecco una guida che parte da zero.**

L'esempio che seguirò a spiegare fa riferimento al sistema operativo Linux distribuzione Red Hat, ma cambia poco o niente per le altre distribuzioni. Al momento che scrivo questo testo la versione di Apache corrente è la 2.0.44 .

## >> Preparativi

Come prima cosa bisogna entrare nella console del sistema operativo Linux, e **la prima operazione da fare è disinstallare la versione installata sul vostro sistema**. In molte distribuzioni Linux infatti è già presente una versione di Apache, ma conviene installarne una nuova (l'ultima), per ottenere miglioramenti in funzionalità, stabilità e sicurezza. Nel caso della distribuzione Linux Red Hat per disinstallare un programma si usa il comando

```
rpm -a apache
```

(in Debian si fa apt-get remove apache )

Disinstallato il vecchio Apache, si deve scaricare il nuovo (dal sito ufficiale www.apache.org); normalmente si trova un file in formato compresso (httpd-2.0.44.tar.gz). Supponiamo ora di copiarlo per esempio nella cartella /usr/local/src/

```
cp httpd-2.0.44.tar.gz
/usr/local/src/
```

dopo esserci spostati nella directory dove lo si è copiato (cd /usr/local/src), lo si deve decomprimere:

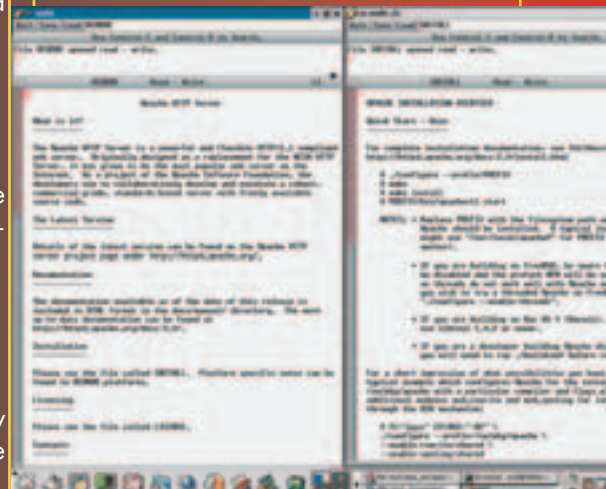
```
tar -zxvf httpd-
2.0.44.tar.gz
```

questo comando creerà la directory ./httpd-2.0.44 dove sono contenuti i file sorgenti di apache.

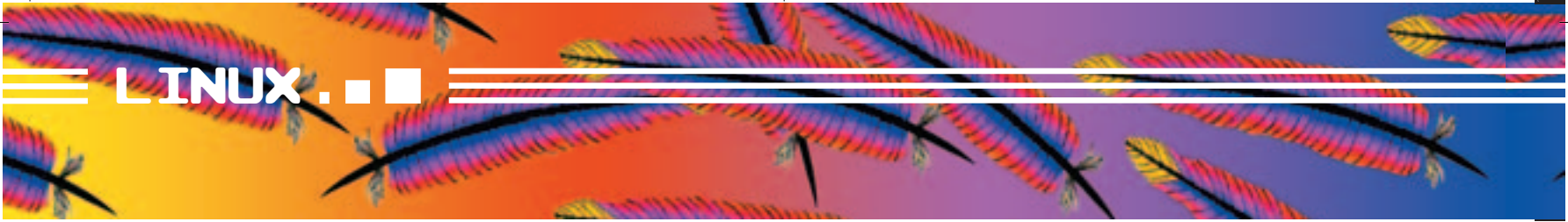
## >> Installazione

Ora entriamo in nella cartella appena creata…

```
cd httpd-2.0.44
```

…e iniziamo con l'installazione vera e propria. Come buona norma, **conviene sempre leggere i file README e INSTALL** per avere un'idea di come procedere.

Prima di inziare, è bene spendere un po' di tempo nella lettura della documentazione.

Per prima cosa, lanciamo il file per la configurazione dei file, poi da compilare:

```
./configure
```

Dopodiché, si deve lanciare il file per compilare i file di installazione

```
make
```

Durante la compilazione lo schermo mostra i vari passaggi del processo: è tutto normale.

Infine, bisogna installare il programma vero e proprio:

```
make install
```

Se non si specifica una directory, per default verrò installato in /usr/local/apache2. Noi faremo riferimento a questo tipo di installazione.
Nel caso in cui nella vostra distribuzione fosse già presente un precedente server Web, ci sarà un file httpd nella directory /usr/sbin/. Se questo file esiste, **bisognerà eliminarlo e creare un collegamento simbolico al nuovo file nella directory di Apache**. Se questo file non esiste, bisognerà **solo creare il collegamento**.
Per verificare se esiste il file, proviamo a elencarlo con:

```
ls /usr/sbin/httpd
```

Se il risultato è una riga vuota, il file non c'è; diversamente, bisognerà eliminarlo (con privilegi di root), in questo modo:

```
rm /usr/sbin/httpd
```

Per creare il collegamento, digitiamo:

```
ln
/usr/local/apache2/bin/http
d /usr/sbin/httpd
```

Questo serve per poter eseguire httpd (il processo del server Web) da qualunque cartella. La cartella /usr/sbin/ è infatti normalmente inclusa nella variabile di sistema PATH.

Dopo l'installazione, bisogna ripristinare il collegamento corretto con httpd.

## >> Configurazione

Installato Apache, ora bisogna configurarlo. Una perfetta configurazione per ottenere un server robusto e affidabile dipende dalla bravura e conoscenza dell'installatore (le opzioni di configurazione sono tantissime). Qui ci limiteremo alla configurazione di base, in modo che funzioni.
Tutto il funzionamento di Apache è regolato dal suo file di configurazione, un file di testo che si trova (nel nostro caso) in usr/local/apache2/conf/httpd.conf.
Per modificare le impostazioni, occorre quindi aprire questo file in un editor di testo. Per esempio, se si usa vi, si può digitare:

```
vi
/usr/local/apache2/conf/htt
pd.conf
```

Per una maggiore comprensibilità, il file di configurazione di Apache comprende già tutte le opzioni, **ma sono disattivate**. Noterete che ogni riga del file di testo inzia con il simbolo #. Questo simbolo indica un commento; **se i comandi sono preceduti da #, vengono quindi ignorati** (si dice che sono "commentati"). Modificare la configurazione in molti casi si riduce quindi alla eliminazione del simbolo # all'inizio della riga, in modo da rendere attivi i comandi seguenti.
Per iniziare, supponiamo che il nostro computer si chiami 'MyWeb', con indirizzo IP 127.0.0.1, che i file del sito sono nella cartella '/MioSito/', e infine che la home page sia costituita dal file '/MioSito/index.html' (da qui in avanti, ci riferiremo a questo esempio). Per impostare un nome al sito basta editare il file /etc/hosts; se questo non è impostato, la macchina si chiama "localhost". Basterà sostituire questo nome con 'MyWeb'. Il formato delle righe è il seguente:

```
IP      NOME    DOMINIO
127.0.0.1    MioSito
localhost.localdomain
```

Aperto il file httpd.conf con un editor di testo, vanno configurate le seguenti voci (togliendo il #):

```
Listen 127.0.0.1:80
```

In questo modo, il demone httpd (il server web) si metterà in ascolto sulla porta 80, quella di default dei server web. A volte capita che ci siano due Listen; per impostare l'ip, mettete il cancelletto davanti alla seconda riga e modificate l'ip alla prima.

```
ServerAdmin boymix81@libero.it
```

Questo parametro serve per indicare l'indirizzo email del webmaster, che potrà essere contattato in caso di problemi. Questo indirizzo comparirà per esempio nelle pagine di errore.

```
ServerName MyWeb:80
```

La nostra macchina avrà un nome su

28_29_hj23_apac 8-04-2003 10:42 Pagina 31

cui sarà contattato il server Web quindi senza dover specificare ogni volta l'ip,

```
DocumentRoot "/MioSito"
```

In questo punto del file di configurazione di Apache si imposta la directory principale del server.

Questo è il comando che indica ad Apache la directory dove sono le pagine web del nostro sito da attivare.

```
<Directory "/MioSito">
```

Appena sotto, bisogna rispecificare la directory.

In seguito si possono specificare i nomi delle pagine da aprire in modo predefinito quando viene richiesta una directory del sito. Normalmente questa pagina è index.html, ma si possono aggiungere altri nomi o estensioni, per esempio index.shtml, indice.html, in questo modo:

```
DirectoryIndex index.html
index.shtml indice.html
```

Tutti i parametri da configurare sono stati indicati nell'ordine in cui li troverete nel file.

## >> Avviare Apache

Per avviare il server Web, dopo aver salvato il file di configurazione, bisognerà dare il comando **httpd** (con privilegi di root).

Per vedere se funziona, basterà aprire un browser qualunque e digitare http://MyWeb. Se tutto è a posto, vedrete la vostra homepage!

Nel prossimo numero vedremo come far partire automaticamente Apache all'avvio di Linux e un po' di altre opzioni di configurazione.

Se tutto va bene, dovreste vedere la vostra bella (ahem...) pagina Web.

**boymix81@libero.it.**

## Alcuni link interessanti...

http://jgo.local.net/LinuxGuide/
http://www.pluto.linux.it/ildp/LDR/ldr.html
http://www.a2.prosa.it/a21.html